

hp StorageWorks

edge switch 2/32 product manager user guide

Part Number: AA-RS2HB-TE

Second Edition (January 2003)

This guide provides an introduction and an overview of the StorageWorks Edge Switch 2/32 Product Manager. It also explains how to use Edge Switch 2/32 features to monitor, manage, and configure the Switch. Finally it describes how to use StorageWorks Edge Switch 2/32 logs and maintenance features.



i n v e n t

© Hewlett-Packard Company, 2003. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Microsoft, MS-DOS, Windows, and Windows 2000 are trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

edge switch 2/32 product manager user guide

Second Edition (January 2003)

Part Number: AA-RS2HB-TE

Contents

About This Guide

Intended Audience	ix
Related Documentation	ix
Document Conventions	x
Symbols in Text	x
Symbols on Equipment	xi
Rack Stability	xii
Getting Help	xii
HP Technical Support	xii
HP Website	xiii
HP Authorized Reseller	xiii

Product Manager Overview

Managing the Edge Switch 2/32	1-1
Menu Options	1-2
High-Availability Fabric Manager (HAFM)	1-2
View Tabs	1-2
Product Menu	1-3
Fabrics Menu	1-3
View Menu	1-3
Configure Menu	1-4
Logs Menu	1-4
Maintenance Menu	1-5
Help	1-5
Product Manager	1-5
View Tabs	1-5
Product Menu	1-5
Configure Menu	1-6
Logs Menu	1-7

Maintenance Menu	1-7
Help Menu	1-8
Product Manager Description	1-8
Using the Product Manager	1-11
Using Dialog Boxes	1-11
Illustrations Used in this Manual	1-11
Keyboard Navigation	1-11
Log Into the HAFM	1-12
Opening the Product Manager	1-14
Window Layout and Function	1-15
Menu Bar	1-15
View Tabs	1-25
View Panel	1-25
Status Bar	1-32
Closing the Product Manager	1-33
User Rights	1-34
User Rights for Specific Functions	1-35
Backing Up and Restoring Product Manager Data	1-37
Restoring Data to the HAFM server	1-38
Using QuikSync	1-38

Monitoring and Managing the Switch

Hardware View	2-1
Identifying FRUs	2-1
Monitoring Switch Operation	2-2
Switch Status Table	2-2
Status Bar Status Indicator	2-4
Monitoring Hardware Operation	2-4
Front View	2-5
Rear View	2-7
Obtaining Hardware Information	2-8
Displaying FRU Information	2-8
Displaying Port Information	2-8
Displaying Switch Information	2-12
Using Menu Options	2-13
Switch Menu	2-13
Port Menu	2-16

Port List View	2-21
Menu Options	2-23
FRU List View	2-24
Node List View	2-25
Menu Options	2-27
Displaying Node Properties	2-28
Performance View	2-30
Menu Options	2-30
Bar Graph Display	2-31
Port Statistics	2-32
Statistics Description	2-32
Troubleshooting Tips	2-35
Button Functions	2-36
Port Operational States	2-36
Link Incident Alerts	2-39
Threshold Alerts	2-40

Configuring the Switch

Configure Identification	3-1
Procedure	3-2
Configure Switch Operating Parameters	3-3
Switch Parameters	3-4
Domain ID	3-4
Rerouting Delay	3-5
Domain RSCNs	3-6
Operating Mode	3-6
Configure Fabric Operating Parameters	3-6
Fabric Parameters	3-8
BB_Credit	3-8
R_A_TOV	3-8
E_D_TOV	3-8
Switch Priority	3-8
Configure Ports	3-10
Procedure (Open Systems mode)	3-12
Procedure (S/390 mode)	3-14
Configure Port Addresses (S/390 mode only)	3-15
Parameters	3-15
Procedure	3-18

Manage Stored Address Configurations	3-19
Procedure	3-19
Configure SNMP	3-21
Procedure	3-22
Configure Optional Features.	3-23
Configure Feature Key	3-24
Procedure	3-24
Configure Date and Time	3-26
Procedure	3-26
Configure Threshold Alerts	3-28
Procedure	3-29
Create New Alert.	3-29
Modify an Alert	3-34
Activate or Deactivate Alerts	3-34
Delete Alerts	3-35
Export Configuration Report	3-35
Procedure	3-36
Enable Web Server.	3-37
Enable Telnet	3-37
Backing Up and Restoring Configuration Data	3-37

Using Logs

Using Logs	4-1
Button Function	4-1
Expanding Columns.	4-2
Sorting Entries	4-2
Audit Log	4-3
Event Log	4-5
Link Incident Log.	4-7
Threshold Alert Log	4-8

Using Maintenance Features

Run Port Diagnostics	5-1
Swap Ports	5-1
Procedure.	5-1
Collect Maintenance Data.	5-2
Execute an IPL	5-3
Set Online State	5-4

Manage Firmware Versions	5-5
Enable E-Mail Notification	5-6
Enable Call-Home Notification	5-6
Backup and Restore Configuration	5-7
Backup	5-7
Restore	5-8
Reset Configuration	5-9
Procedure	5-9

Optional Features

FICON Management Server	6-1
Installation	6-1
Configuring the FICON Management Server	6-2
Procedure	6-4
Open Systems Management Server	6-5
Installation	6-5
Configuring the Open Systems Management Server	6-5
SANtegrity Features	6-6
Fabric Binding	6-6
Enable/Disable and Online State Functions	6-7
Switch Binding	6-7
Configuring Switch Binding - Overview	6-7
Enable/Disable Switch Binding	6-8
Editing the Switch Membership List	6-9
Enable/Disable and Online State Functions	6-11
Zoning with Switch Binding Enabled	6-12
Enterprise Fabric Mode	6-13
Fabric Binding	6-13
Switch Binding	6-13
Rerouting Delay	6-13
Domain RSCNs	6-14
Insistent Domain Identification (ID)	6-14

Product Manager Messages

Glossary

Index

Figures

1-1	Switch management components on LAN	1-9
1-2	HAFM icon	1-12
1-3	Main HAFM window	1-13
1-4	Edge Switch 2/32 icon	1-14
1-5	Edge Switch 2/32 Product Manager window (Hardware view)	1-14
1-6	Port List View	1-27
1-7	FRU List View	1-28
1-8	Node List View	1-29
1-9	Performance View	1-30
2-1	Monitoring hardware operation — Edge Switch 2/32 Hardware view	2-5
2-2	FRU Properties dialog box	2-8
2-3	Port Properties dialog box	2-9
2-4	Switch Properties dialog box	2-12
2-5	Configure Date and Time Periodic Synchronization dialog box	2-15
2-6	Configure date and time manually	2-15
2-7	Set Online State dialog box (Offline)	2-16
2-8	Set Online State dialog box (Online)	2-16
2-9	Bind WWN dialog box	2-19
2-10	Clear Threshold Alert(s) dialog box	2-20
2-11	Port List View	2-21
2-12	FRU List View	2-24
2-13	Node List View	2-25
2-14	Node Properties dialog box	2-28
2-15	Performance view	2-30
3-1	Configure Identification dialog box	3-2
3-2	Configure Switch Parameters dialog box	3-3
3-3	Configure Fabric Parameters dialog box	3-7
3-4	Configure Ports dialog box	3-12
3-5	Configure Ports dialog box (S/390 Mode)	3-14
3-6	Prohibited Port Connection symbol	3-16
3-7	Configure Addresses dialog box	3-18

3-8	Address Configuration Library dialog box	3-19
3-9	Configure SNMP dialog box.	3-22
3-10	Configure Feature Key dialog box	3-24
3-11	New Feature Key dialog box	3-25
3-12	Configure Date and Time Periodic Synchronization dialog box	3-27
3-13	Configure date and time manually	3-27
3-14	Configure Threshold Alerts dialog box	3-29
3-15	New Threshold Alerts dialog box - first screen	3-30
3-16	New Threshold Alerts dialog box - second screen	3-31
3-17	New Threshold Alerts dialog box - third screen	3-32
3-18	New Threshold Alerts dialog box - summary screen	3-33
3-19	Configure Threshold Alerts dialog box - alert activated.	3-33
3-20	Export Configuration dialog box	3-36
4-1	Save dialog box.	4-2
4-2	Audit Log	4-3
4-3	Event Log	4-5
4-4	Hardware Log	4-6
4-5	Link Incident Log	4-7
4-6	Threshold Alert Log	4-8
5-1	Swap Ports dialog box.	5-2
5-2	IPL Confirmation dialog box	5-3
5-3	Set Online State dialog box (Offline)	5-5
5-4	Set Online State dialog box (Online)	5-5
5-5	Backup and Restore dialog box	5-7
6-1	Configure FICON Management Server dialog box	6-4
6-2	Configure Open Systems Management Server dialog box	6-5
6-3	Switch Binding State Change dialog box	6-8
6-4	Switch Binding Membership List dialog box	6-10

Tables

1-1	Operating Status — Status Bar and Switch Status	1-32
1-2	User rights for Product Manager functions.	1-35
2-1	Port States and Indicators	2-36
6-1	Available Code Pages	6-3
A-1	StorageWorks Edge Switch 2/32 Product Manager Messages	A-1

About This Guide

This installation guide provides information to help you:

- Set up the Edge Switch 2/32.
- Configure the Edge Switch 2/32.
- Manage the Edge Switch 2/32.
- Contact technical support for additional assistance.

Intended Audience

This book is intended for use by administrators who are experienced with the following:

- Fibre Channel technology
- StorageWorks Fibre Channel Switches by Hewlett-Packard

Related Documentation

For a list of corresponding documentation, see the Related Documents section of the *hp StorageWorks edge switch release notes*.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks website: <http://h18006.www1.hp.com/storage/saninfrastructure.html>.

For information about Fibre Channel standards, visit the Fibre Channel Association website, located at <http://www.fibrechannel.org>.

Document Conventions

The conventions included in [Table 1](#) apply.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key names, menu items, buttons, and dialog box titles	Bold
File names, application names, and text emphasis	<i>Italics</i>
User input, command names, system responses (output and messages)	Monospace font COMMAND NAMES are uppercase unless they are case sensitive
Variables	<i>Monospace, italic font</i>
Website addresses	Sans serif font (http://thenew.hp.com)

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.



CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

These icons may be located on equipment in areas where hazardous conditions may exist.



Any surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.



Any RJ-45 receptacle marked with these symbols indicates a Network Interface Connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



Power Supplies or Systems marked with these symbols indicate the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the system.



Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal INJURY or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Rack Stability



WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
 - The full weight of the rack rests on the leveling jacks.
 - The stabilizing feet are attached to the rack if it is a single rack installations.
 - The racks are coupled together in multiple rack installations.
 - A rack may become unstable if more than one component is extended for any reason. Extend only one component at a time.
-

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: <http://thenew.hp.com>.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

NOTE: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: <http://thenew.hp.com/country/us/eng/support.html>.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: <http://thenew.hp.com/country/us/eng/prodserv/storage.html>. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP Authorized Reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers:
<http://thenew.hp.com>.

Product Manager Overview

This chapter is an introduction and overview of the Edge Switch 2/32 *Product Manager* application. It is intended as a quick reference for using features available through the main **Product Manager** window.

Managing the Edge Switch 2/32

These options are available for managing the Edge Switch 2/32 through a user interface:

- The *Product Manager* application installed on an High Availability Fabric Manager (HAFM) server. Access to the Product Manager must be through the HAFM applications. These applications are installed on the HAFM server.
- The Embedded Web Server (EWS) interface. Using a browser-capable PC with an internet connection to the Switch, you can monitor and manage the Switch through the web server interface embedded in the Switch firmware. The interface provides a GUI similar to the *Product Manager* application and supports Switch configuration, statistics monitoring, and basic operation.

To launch the Embedded Web Server interface, enter the Switch's IP address as the internet uniform resource locator (URL) into any standard browser. Enter a user name and password at a the login screen. The browser then becomes a management console. Refer to the web server interface online help for details on use.

NOTE: The default user name for the right to view status and other information is "operator." The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is "administrator." The default password for both user names is "password."

- The command line interface (CLI). The CLI allows you to access many HAFM and Product Manager functions while entering commands during a Telnet session with the Switch. The primary purpose of the CLI is to automate management of a large number of Switches using scripts. The CLI is not an interactive interface; no checking is done for pre-existing

- conditions and no prompts display to guide users through tasks. Refer to the *hp StorageWorks CLI reference guide for directors and edge switches* .
- Management using simple network management protocol (SNMP). An SNMP agent is implemented through the *SDCM* application that allows administrators on SNMP management workstations to access Switch management information using any standard network management tool. Administrators can assign internet protocol (IP) addresses and corresponding community names for up to six SNMP workstations functioning as SNMP trap message recipients.

This manual provides details on the *Product Manager* application for the Edge Switch 2/32 only. Use this manual for the Product Manager installed on an HAFM server. For information on the Embedded Web Server interface, see the *hp StorageWorks embedded web server user guide*; for information on the CLI, see the *hp StorageWorks CLI reference guide for directors and edge switches* .

Menu Options

This user's guide provides information on the Edge Switch 2/32 *Product Manager* application only. Information on the *HAFM* application is provided in the *hp StorageWorks ha-fabric manager user guide*. Following are lists of options available from the menu bar in both applications. References are provided to the correct publication for detailed information on these options.

High-Availability Fabric Manager (HAFM)

Following are options available through the HAFM. For more information, refer to Chapter 3 of the *hp StorageWorks ha-fabric manager user guide*.

View Tabs

- Products
- Fabrics

Product Menu

- New
- Open
- Delete
- Modify
- Properties
- Logout
- Exit

Fabrics Menu

- Rename
- Persist Fabric Topology
- Unpersist Fabric Topology
- Export Fabric Topology
- Show Route
- Hide Route
- Show Zone Members
- Show View Port
- Show Fabric Tree
- Enterprise Fabrics Mode (menu only active if SANtegrity is installed)
- Fabric Binding (menu only active if SANtegrity is installed)

View Menu

- User Sessions
- Zoom
 - In
 - Out
 - Default
 - Fit in View

- Arrange Icons
 - By Name
 - By Severity
- Layout Icons
 - Circular
 - Spring
- Center in Topology
- Clear ISL Alert
- Clear All ISL Alerts
- Enable Fly Over Display

Configure Menu

- Users
- Nicknames
- Sessions
- SNMP Agent
- Activate Zone Set
- Zoning Library
- Advanced Zoning
 - Deactivate Zone Set
 - Configure Default Zone

Logs Menu

- Audit Log
- Event Log
- Session Log
- Product Status Log
- Fabric Log

Maintenance Menu

- Configure E-Mail
- Test Remote Notification
- Configure Ethernet Events
- Configure Call Home Event Notification

Help

- Contents
- About

Product Manager

Following are options available through the *Product Manager* application for your Switch. For more information on these options, refer to [Menu Bar on page 1-15](#) in this manual.

View Tabs

- Hardware
- Port List
- Node List
- Performance
- FRU List

Product Menu

- Port (options available when port is selected)
 - Port Properties
 - Node Properties
 - Port Technology
 - Block Port
 - Enable Beaconsing
 - Port Diagnostics

- Channel Wrap (S/390 mode only)
 - Swap Ports (S/390 mode only)
 - Clear Link Incident Alert(s)
 - Reset Port
 - Port Binding
 - Clear Threshold Alerts(s)
 - Display Options (Nickname and World Wide Name)
- FRU
 - Open Port Card View
 - FRU Properties (based upon which FRU was selected)
 - Switchover (Director only)
 - Block All Ports
 - Unblock All Ports
 - Diagnostics
- Clear System Error Light
- Enable Unit Beacons
- Properties
- Close

Configure Menu

- Identification
- Operating Mode
- Operating Parameter
 - Switch Parameters
 - Fabric Parameters
- Ports

- Addresses (S/390 mode only)
 - Active
 - Stored
- SNMP Agent
- Management Server (only active if a management server feature is installed)
- Features
- Date/Time
- Threshold Alert
- Export Configuration Report
- Enable Web Server
- Enable Telnet

Logs Menu

- Audit Log
- Event Log
- Hardware Log
- Link Incident Log
- Threshold Alerts Log

Maintenance Menu

- Port Diagnostics
- Swap Ports (S/390 mode only)
- Data Collection
- IPL
- Set Online State
- Firmware Library
- Enable E-Mail Notification
- Enable Call Home

- Backup and Restore Configuration
- Reset Configuration

Help Menu

- Contents
- About

Product Manager Description

The Product Manager for the Edge Switch 2/32 is a Java-based graphical user interfaces (GUI) that provides in-depth management, configuration, and monitoring functions for individual Switches and their field-replaceable units (FRUs). Although the Product Manager is accessed from the *HAFM* application, it is a separate application.

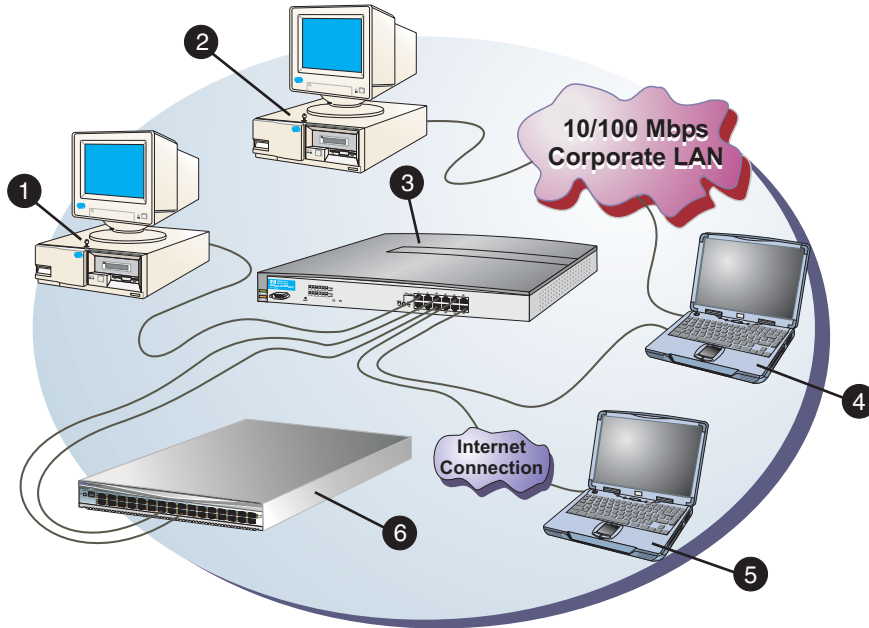
In contrast to the Product Manager, the HAFM enables administrators to monitor operational status for all products and Fibre Channel fabrics managed by an HAFM server. The HAFM also provides tools to administer user and product access to the HAFM and Product Manager. Refer to the *hp StorageWorks ha-fabric manager user guide*.

The Product Manager provides graphical views of Switch hardware components and displays of component status. By positioning the cursor on icons, graphics, panels, and other visual elements in these views and clicking the left or right mouse button, you can quickly manage and monitor the Switch on your network.

Access the Switch Product Manager by double-clicking any Switch product icon on the HAFM's **Products** or the **Topology Fabrics** views.

[Figure 1–1 on page 1–9](#) illustrates Switch management components. The figure shows the following elements:

You can install the *HAFM* and *Product Manager* applications on remote workstations, as shown in [Figure 1–1](#), using any standard web browser. For instructions, refer to the appendix in the *hp StorageWorks ha-fabric manager user guide* that pertains to the operating system of your workstation.



SHR-2314b

- | | |
|-------------------------------|---------------|
| ❶ SNMP management workstation | ❷ HAFM server |
| ❸ Remote user workstation | ❹ Web browser |
| ❺ HP Ethernet hub | ❻ Switch |

Figure 1–1: Switch management components on LAN

Using the Product Manager, you can:

- Back up and restore configuration data.
- Change operating mode between S/390 and open systems modes.
- Clear the system error indicator.
- Configure extended distance buffering for ports.
- Configure Fibre Channel operating parameters for the Switch, such as BB_Credit, R_A_TOV, E_D_TOV, preferred domain ID, Switch priority, and rerouting delay.
- Configure individual ports with a port name describing the node attached to the port.
- Configure keys for new features.

- Configure LIN alerts.
- Configure Port Binding.
- Configure port addresses (S/390 mode only)
- Configure Nickname to display instead of WWN for the Switch and attached devices.
- Configure SNMP trap recipients and community names.
- Configure the FICON and Open Systems Management Server Features (if installed)
- Configure the Switch name, location, description, and contact person.
- Control individual Fibre Channel ports by blocking/unblocking operation, enabling LIN alerts and port binding, setting data speeds, and running internal and external loopback diagnostics.
- Display FRU properties such as the FRU name, physical position in the Switch (chassis slot number), active failed state, part number, and serial number.
- Display information for individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.
- Display information on nodes attached to ports.
- Display port performance and statistics.
- Display vital product data for the Switch, such as the system name, description, contact person, location, status, model number, firmware and EC level, and manufacturer.
- Enable beaconing for ports and the Switch unit.
- Enable channel wrap mode (S/390 mode only).
- Maintain a port address library (S/390 mode only).
- Monitor the operational status of the Switch and each of its hardware field-replaceable units.
- Perform an initial program load (IPL).
- Perform maintenance tasks for the Switch including maintaining firmware levels, administering the call-home feature, accessing the Switch logs, and collecting data to support failure analysis.
- Reset port operation.
- Run port diagnostics.

- Set the date and time on the Switch.
- Swap addresses between ports (S/390 mode only)
- Use standard keyboard navigation through dialog boxes (for example, using the **Tab**, **arrow**, and **Enter** keys).

Using the Product Manager

This section provides a general overview of the Product Manager and its functions. For details on performing specific tasks and using specific dialog boxes, refer to the appropriate chapters in this manual.

Using Dialog Boxes

Buttons such as **OK**, **Activate**, and **Close** or **Cancel** initiate functions in a dialog box. There is a difference between the **OK** and **Activate** buttons. The **OK** button saves the data you entered and closes the dialog box. The **Activate** button saves the data you entered without closing the dialog box, unless there is a **Close** button. In this case, **Activate** saves the information without closing the box. There is also a difference between the **Close** and **Cancel** buttons. The **Close** button closes the dialog box and saves the data you entered. The **Cancel** button cancels the operation and closes the dialog box without saving the information you entered.

Illustrations Used in this Manual

Figures containing HAFM and Product Manager screens in this manual are included for illustration purposes only. These illustrations may not match exactly what you see through your server or workstation. Title bars have been removed from the illustrations and fields in the illustrations may contain different data than in screens displayed on your system.

Keyboard Navigation

Use standard keyboard navigation in dialog boxes. For example, use the **Tab**, arrow, and backspace keys to move through dialog box fields and the **Enter** key to perform default button functions.

Log Into the HAFM

To open the Product Manager, you must first log into the HAFM.

1. Perform one of the following steps:
 - If you are using the HAFM server, the *HAFM* application automatically starts when you power on or reboot the HAFM server. If you reboot or Switch on the HAFM server and the **HAFM** login screen displays, skip to step 3 to log in.
 - If you are using a remote user workstation, follow steps 2 through 5.
 - If the **HAFM** window is already displayed, skip to [Opening the Product Manager on page 1-14](#).
2. Perform one of the following steps if you are using a remote user workstation (a network PC with a remote client installed), and the **HAFM** login screen or **HAFM** window is not displayed. If the login screen is displayed, go to step 3.
 - Start the *HAFM* application and display the login screen by double-clicking the **HAFM** icon on the desktop.



Figure 1–2: HAFM icon

The **HAFM** login screen displays

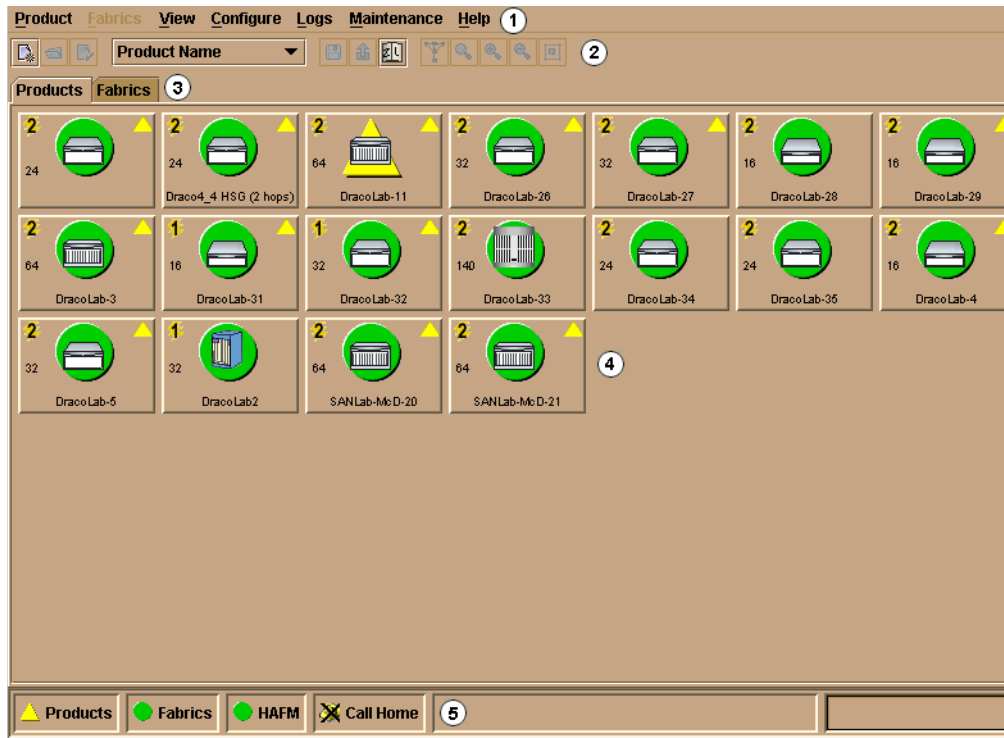
- If the **HAFM** window is open ([Figure 1–3 on page 1-13](#)) and you need to log in as another user or access a different HAFM server, choose **Logout** from the **Product** menu on the menu bar to display the login screen. Go to step 3.
3. When the HAFM login screen displays, enter your user name and password. The default user name is Administrator and password is password unless changed by your system administrator.

NOTE: The default user name for the right to view status and other information is “operator.” The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is “administrator.” The default password for both user names is “password.”

NOTE: If the HAFM window is open ([Figure 1–3 on page 1-13](#)) and you need to log in as another user or access a different HAFM Server, choose **Logout** from the **Logout** or **Logout/Exit** menu on the menu bar to display the login screen.

4. In the **HAFM Server** field on the login screen, choose the HAFM server to which you want to connect. Note that if you are logging into an HAFM server locally, `localhost` is the HAFM server name. Type in the network address of the server if it is not in the list.
5. Click **Activate** or press the **Enter** key on your keyboard.

The main **HAFM** window displays showing the **Product** view (Figure 1–3).



- | | |
|-------------|----------------|
| ❶ Menu Bar | ❷ Main Panel |
| ❸ Tool Bar | ❹ Status Panel |
| ❺ View Tabs | |

Figure 1–3: Main HAFM window

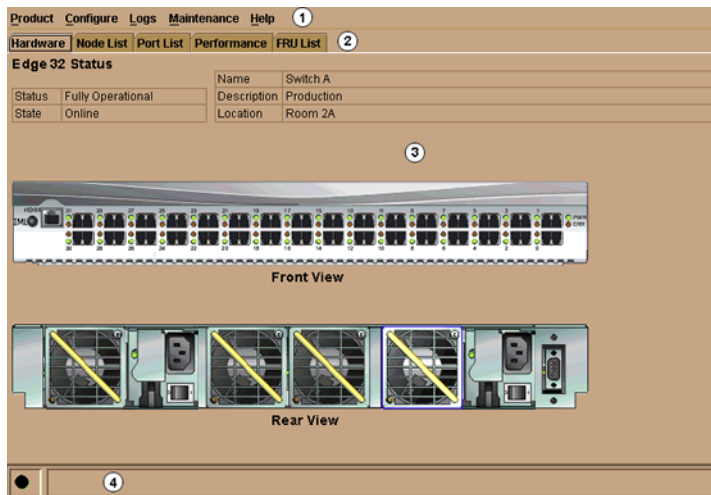
Opening the Product Manager

To open the Product Manager, double-click the product icon in the **Product** view or right-click the icon and choose **Open**.



Figure 1–4: Edge Switch 2/32 icon

The Product Manager displays showing the default **Hardware** view. [Figure 1–5](#) shows the **Edge Switch 2/32 Hardware** view.



- ❶ Menu Bar
- ❷ View Tabs
- ❸ View Panel
- ❹ Status Bar

Figure 1–5: Edge Switch 2/32 Product Manager window (Hardware view)

NOTE: The **HAFM** window is still available as a separate window. You can drag the **Product Manager** window away from the **HAFM** window and view both windows on your PC desktop or minimize one or both of them to icons if desired. You can have a maximum of four **Product Manager** windows open concurrently.

Window Layout and Function

The main **Product Manager** window is divided into four main areas as shown in [Figure 1–5 on page 1-14](#): menu bar, view tabs, view panel, and status bar. Use features in these panels to configure Switch operation, monitor performance, and access maintenance features.

Menu Bar

The menu bar on the **Product Manager** window displays tabs for the following menus:

- Product
- Configure
- Logs
- Maintenance
- Help

Click one of the tabs to display a list of menu options. Click an option to open a dialog box that allows you to perform configuration and maintenance tasks and view logs. If a menu option contains a check box, click in the box to add a check mark and enable a function. Click a check box containing a check mark to remove the check mark and disable the function.

Product Menu

Choose one of the following options from the **Product** menu.

Port

This provides a secondary port menu only when the **Hardware** view, **Port List** view, or **Performance** view displays in the view panel. To use this menu for a specific port, click a port in the **Hardware** view, a port's row in the **Port List** view, or a port's bar graph in the **Performance** view. The menu contains options which are identical to those that display when you right-click the port, port row, or port bar graph in those views. For detail on these options refer to [Port Menu on page 2-16](#).

FRU

Click a power supply module or cooling fan module in the **Hardware** view only and choose **FRU** from the **Product** menu to display the **FRU Properties** menu option. This displays the **FRU Properties** dialog box. The **FRU Properties** dialog box can also be displayed by double-clicking on the FRU in the **Hardware** view. These are the same menu option as when you double-click these components in the **Hardware** view. For details on these options refer to [Displaying FRU Information on page 2-8](#).

Clear System Error Light

Choose this to turn off the amber system error LED, located below the green power LED on the Switch front bezel.

Enable Unit Beaconing

Click the check box to toggle unit beaoning on or off. When the check box has a check mark, unit beaoning is on, and the amber system error light on the Switch front bezel blinks to help users locate the actual unit in an equipment room. When you click the check box to remove the check mark, unit beaoning is disabled and the amber LED goes out. You can only enable beaoning if there are no system errors (the system error light is off).

Properties

Click to display the **Switch Properties** dialog box. This dialog box contains the Switch name, description, location, and contact person configured through the **Configure Identification** dialog box. Also included is other product information as detailed in Switch Properties. You can also display this dialog box by double-clicking an area on the illustration in the **Hardware** view, away from a hardware component.

Close

Choose this option to close the **Product Manager** window.

Configure Menu

Click the **Configure** menu on the menu bar to display the following options. For detailed information on using these options, refer to [Chapter 3, Configuring the Switch](#).

Identification

Choose this option to display the **Configure Identification** dialog box. Enter the following information in this dialog box:

- **Name** - Assign a product name. Note that you can set this name as the nickname for the Switch's WWN, using the **Set Name as Nickname** check box. The nickname then displays instead of the WWN in **Product Manager** views.
- **Description** - Assign a unique product description.
- **Location** - Describe the product's location.
- **Contact** - Assign a contact either by name, phone number, or e-mail address.

NOTE: This information displays in the identification table at the top of the **Hardware** view and in the HAFM **Product** view, if the **Product** view is configured to display names.

Switch Operating Parameters

Choose this option to display the **Configure Switch Parameters** dialog box for setting Fibre Channel operating parameters. In this dialog box, you can set preferred domain identification (1 to 31) and make it insistent. You can also enable rerouting delay and domain register for state change notifications (RSCNs). In addition, you can also set the Switch operating mode to S/390 mode or Open Systems mode. The Switch must be offline to configure preferred domain ID and operating mode.

Refer to [Configure Switch Operating Parameters on page 3-3](#) for more information on configuring the Switch priority and rerouting delay.

Fabric Operating Parameters

Choose this option to display the **Configure Fabric Parameters** dialog box for setting fabric operating parameters. In this dialog box, you can set buffer-to-buffer credit (**BB_Credit**) from 1 to 60 (default is 16) and the resource allocation time-out value (**R_A_TOV**) and error detect time-out value (**E_D_TOV**) in tenth-of-a-second increments. In addition, you can set the Switch priority level (**Principal**, **Default**, or **Never Principal**) and the interoperability modes between **Homogenous Fabric** and **Open Fabric 1.0**.

Refer to [Configure Switch Operating Parameters on page 3-3](#) for more information on configuring these parameters for the Switch. The Switch must be offline to configure any fabric operating parameter.

Switch Binding

This submenu provides two options: **Change State** and **Edit Membership List**. Choosing **Change State** displays the **Switch Binding State Change** dialog box where you can activate Switch Binding according to a specific connection policy (**Restrict E_Ports**, **Restrict F_Ports**, or **All Ports**). **Edit Membership List** allows you to create a list of Switches and devices that you want to allow exclusively to attach to Director ports. Switch Binding is an optional feature that requires the SANtegrity feature key. The feature can be installed through the **Configure Feature Key** dialog box. For details, refer to [SANtegrity™ Features on page 6-7](#).

Ports

Choose this option to display the **Configure Ports** dialog box. This dialog box has different functions in S/390 versus open systems.

In S/390 mode, use the dialog box to enable extended distance buffering for 10 to 100km, link incident (LIN) alerts, and port binding for each port.

In open systems mode, for each port you can provide a name, block or unblock operation, configure extended distance buffering for 10 to 100km, enable LIN alerts for each port, define a type (G, F, and E), and enable port binding.

NOTE: Ports are automatically configured as G_Ports if no device is connected, F_Ports if a device is connected, and E_Ports if a Switch is connected. You can enable the rerouting delay feature.

Addresses

S/390 mode only — Choose from two suboptions for active and stored addresses.

Active Addresses — Displays the **Configure Addresses - “Active”** dialog box. Use this dialog box to configure a name, blocked or unblocked state, and prohibited and allowed connection attributes for a port.

Stored Addresses — Displays the **Address Configuration Library**. Use this dialog box to activate, modify, or delete existing address configurations created through the **Active Addresses** dialog box.

SNMP Agent

Choose this option to display the **Configure SNMP** dialog box. Use this dialog box to configure network addresses and community names for up to six SNMP trap recipients. Also authorize write permissions to enable SNMP management stations to modify writable MIB variables. In addition, you can enable authorization traps to be sent to management stations when unauthorized stations request access to Switch SNMP data.

Management Server

Choose this option to display either the **Configure Open Systems Management Server** or **Configure FICON Management Server** dialog box, depending on which feature (if any) is enabled for the Switch. Use this to configure a FICON or open systems inband management program to function with the Switch. To use these procedures, you must have enabled either FICON Management Server or Open Systems Management Server through the **Configure Feature Key** dialog box.

Features

Displays the **Configure Feature Key** dialog box. Use this dialog box to enter a feature key to enable optional features that you have purchased for the Switch.

Date and Time

Choose this option to display the **Configure Date and Time** dialog box. Use this option to set the current date and time in the Switch. When the **Periodic Date/Time Synchronization** check box is checked, the **Date and Time** fields are greyed out (disabled), and the HAFM server date and time periodically synchronizes the Switch date and time. If the **Periodic Date/Time Synchronization** check box is not checked, you can set the date and time in the dialog box fields manually.

Threshold Alert(s)

Choose this option to configure threshold alerts for ports. A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific Switch ports or port types (E_Ports or F_Ports). Using this option, you can configure:

- A name for the alert.
- A threshold type for the alert (Rx, Tx, or either).

- Active or inactive state of the alert.
- Threshold criteria. This includes configuring the threshold as the percent of port traffic capacity utilized (**% utilization**). You must also configure the time interval during which the throughput is measured and the maximum cumulative time that the throughput percentage threshold can be exceeded during this time interval before an alert is generated.

Export Configuration Report

Choose this option to display the **Export Configuration Report** dialog box, which enables you to specify a file name in which to save an ASCII text file containing all current user-definable configuration options in a printable format. Note that this file cannot be read back into the Product Manager in order to set configuration parameters.

Enable Web Server

Choose this option to enable the Embedded Web Server interface on the Switch. Choose the option again to disable the Embedded Web Server interface. When disabled, users at remote workstations cannot access the interface. If enabled, Hewlett-Packard recommends changing the user names and/or passwords from their default values to prevent unauthorized access.

Enable Telnet

Choose this option to enable telnet access to the Switch. Choose the option again to remove disable telnet access. When disabled, users at remote workstations cannot access the Switch through the telnet in order to use the Command Line Interface (CLI) or perform other tasks. If enabled, Hewlett-Packard recommends changing the user names and/or passwords from their default values to prevent unauthorized access.

Logs Menu

Click the **Logs** menu from the menu bar to display the following options. For detailed information on using these dialog boxes, refer to [Using Logs on page 4-1](#).

Audit Log

This log provides a record of all configuration changes made on the Switch. Each entry displays the date and time of the change, a description of the change, the source of the change (such as the HAFM server or SNMP management station), and an identifier for the source, such as the IP address of the HAFM server or SNMP management station.

Event Log

Choose this option to display the Switch event log. This log provides a record of significant events that have occurred on the Switch, such as hardware failures, degraded operation, and port problems. Each entry includes the date and time of the event, a reason code for the event, the severity level, a brief description, and up to 32 bytes of supplementary event data. Refer to the *hp StorageWorks edge switch 2/32 service manual* for more information.

Hardware Log

This log displays information on FRUs inserted and removed from the Switch. Each log entry includes the name of the FRU inserted or removed, the slot position relative to identical FRUs installed, whether the FRU was inserted or removed, the FRU part number and serial number, and the date and time the FRU was inserted or removed.

Link Incident Log

The link incident (LIN) log displays the most recent incidents with their date and time, port number, and description of the incident. A link incident can be one of several conditions detected on a fiber optic link. For a list of events that may cause a link incident to be written to the log, refer to [Link Incident Log on page 4-7](#).

Threshold Alert Log

This log provides notifications of threshold alerts. Besides the date and time that the alert occurred, it also displays information that was configured through the **Configure Threshold Alert(s)** option under the **Configure** menu. This includes the alert name, port for which the alert is configured, the type of alert (transmit throughput, receive throughput, or both), threshold utilization of traffic capacity, minutes the threshold was configured for, and the configured time interval for the threshold. For more details on this log, refer to [Threshold Alert Log on page 4-8](#).

Maintenance Menu

Click the **Maintenance** menu on the menu bar to display the following options. For detailed information on using these dialog boxes, refer to [Chapter 5, Using Maintenance Features](#).

Port Diagnostics

This option displays the **Port Diagnostics** dialog box. Use this dialog box to run internal and external loopback tests on ports. Refer to the *hp StorageWorks edge switch 2/32 service manual* for instructions.

Swap Ports

S/390 mode only. Choose this option to display the **Swap Ports** dialog box. Use this dialog box to swap one port address for another.

Data Collection

This option displays the **Save Data Collection** dialog box. Use this dialog box to collect maintenance data into a file. This file is used by support personnel to diagnose system problems. Refer to the *hp StorageWorks edge switch 2/32 service manual* for instructions.

IPL

Choose this option to initiate an initial program load on the Switch. A dialog box displays to allow you to confirm the IPL. Note that an IPL does not affect any configuration settings done through the Product Manager. Port operation is interrupted during the IPL.

Refer to [Execute an IPL on page 5-3](#) for more information.

Set Online State

Choose this option to display the **Set Online State** dialog box. Use this dialog box to change the online state of the Switch to offline or online.

Firmware Library

Choose this option to display the **Firmware Library** dialog box. This dialog box displays all firmware versions currently installed on the HAFM server that can be downloaded to Directors. Use this dialog box to add a new firmware version to the HAFM server hard disk, modify the description displayed for an existing version, delete a version from the PC, or download (send) a version for operation on a Switch. For additional information on using this option, refer to the *hp StorageWorks edge switch 2/32 service manual*.

Enable E-Mail Notification

The Simple Mail Transfer Protocol (SMTP) server and e-mail recipient addresses are configured in the *HAFM* application (not in the Switch's Product Manager). E-mail notification is also initially enabled in the HAFM for all Directors managed by the HAFM. Note, however, that the **E-Mail Notification** option on the Product Manager's **Maintenance** menu must be enabled (checked) for e-mail notification to occur for the specific Switch.

The default setting for the **Enable E-Mail Notification** function is enabled (checked). To disable the function, choose **Enable E-Mail Notification** from the **Maintenance** menu to clear the check box.

For additional information on using this option, refer to [Enable E-Mail Notification on page 5-6](#).

Enable Call Home Notification

NOTE: The default setting for the **Enable Call Home Notification** function is disabled (unchecked).

Choose **Enable Call Home Notification** from the **Maintenance** menu to enable the call-home function for the Switch.

The parameters of the call-home feature are configured in Windows. Refer to the *hp StorageWorks HAFM server installation guide* for instructions.

Backup & Restore Configuration

Choose this option to save the product configuration stored on the Switch to the HAFM server hard disk or to restore the configuration data from the HAFM server. Only a single copy of the configuration is kept on the server.

This backup is primarily for single-CTP systems, where a backup is needed to restore the configuration data to a replacement CTP card. You cannot modify the location or the file name of the saved configuration.

NOTE: You can only restore the configuration to a Switch with the same IP address.

For additional information on using this option, refer to [Backing Up and Restoring Configuration Data on page 3-37](#).

Reset Configuration

Choose this option to reset all Switch configuration data back to the factory defaults. A confirmation dialog box displays with a warning upon choosing the option. For additional information on using this option, refer to [Reset Configuration on page 5-9](#).



CAUTION: This operation resets all configuration including any optional features that have been installed. You will need to re-enter your feature key to enable all optional features after resetting the configuration.

Help Menu

Click the **Help** menu on the menu bar to display the following options.

Contents

Choose this option to display the **Help** window. The **Help** window contains **Contents**, **Index**, and **Glossary** buttons and hypertext-linked items to help you quickly navigate through information. Use the forward (>) and back (<) buttons to scroll forward and backward through the displayed help frames. Exit the help feature at any time by clicking the **Close** selection at the top of the **Help** window.

About

Choose this option to display the version number for the Product Manager and copyright information.

View Tabs

Click one of the view tabs across the top of the **Product Manager** window to display the following views in the **View** panel.

- Hardware
- Node List
- Port List
- Performance
- FRU List

View Panel

Views, selected from the **View** tabs, display under the tabs in the **View** panel.

Hardware View

The **Hardware** view is the default view that displays in the view panel when you open the Switch Product Manager. To return to this view from another view, click the **Hardware** view tab. Refer to [Figure 1–5 on page 1-14](#) for an example of this view.

In the **Hardware** view, colored indicators reflect the status of actual LEDs on the Switch FRUs. The status bar displays a symbol to represent the most degraded status currently reported by any of the Switch FRUs. For example, for a port failure, indicated by a blinking red and yellow diamond on a port, a yellow triangle displays on the status bar to indicate a degraded condition. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a blinking red and yellow diamond, which indicates a failure requiring immediate attention. For an explanation of the different status symbols and the reasons they display in the **Hardware** view or **Port List** view, refer to the table under [Monitoring Hardware Operation on page 2-4](#).

Switch Menu

Double-click the Switch graphic away from a FRU to display the **Switch Properties** dialog box. Right-click a hardware graphic away from a FRU to display the following options:

- Switch Properties
- Enable Unit Beaconing
- Clear System Error Light

- IPL Switch
- Set Switch Date and Time
- Set Switch Online State

For details on menu options, refer to [Switch Menu on page 2-13](#).

For details on navigating and monitoring via the **Hardware** view, refer to [Hardware View on page 2-1](#).

Port Menu

Double-click a port to display the **Port Properties** dialog box. Right-click a port to display the following options:

- Port Properties
- Node Properties
- Port Technology
- Block Port
- Enable Beaconsing
- Channel Wrap (S/390 mode only)
- Swap Ports (S/390 mode only)
- Port Diagnostics
- Clear Link Incident Alert(s)
- Reset Port
- Port Binding
- Clear Threshold Alert(s)

Note that these same options are available when you click a port on the **Hardware** view and choose the port secondary menu from the **Product** menu on the menu bar.

NOTE: For **Node Properties**, if a node is not logged in, a message box displays indicating that node information is not available.

For details on menu options, refer to [Port Menu on page 2-16](#).

For details on navigating and monitoring via the **Hardware** view, refer to [Hardware View on page 2-1](#).

Port List View

Choose the **Port List** view tab. A table listing the port number, port name, port address (S/390 mode only), the block/unblock configuration, operating state, operating speed, port type, and alert condition displays in the view panel. [Figure 1–6](#) shows an example of the **Port List** view.

Product Configure Logs Maintenance Help							
Hardware Port List Node List Performance FRU List							
#	Name	Block Config	State	Type	Operating Speed	Alert	
0		Unblocked	Online	E Port	2 Gb/sec		
1		Unblocked	Online	E Port	2 Gb/sec		
2		Unblocked	No Light	F Port	1 Gb/sec		
3		Unblocked	Online	F Port	2 Gb/sec		
4		Unblocked	No Light	G Port	Not Established		
5		Unblocked	No Light	G Port	Not Established		
6		Unblocked	Online	F Port	1 Gb/sec		
7		Unblocked	No Light	G Port	Not Established		
8		Unblocked	Online	F Port	1 Gb/sec		
9		Unblocked	Online	F Port	1 Gb/sec		
10		Unblocked	No Light	G Port	Not Established		
11		Unblocked	Online	F Port	2 Gb/sec		
12		Unblocked	No Light	G Port	Not Established		
13		Unblocked	Online	F Port	2 Gb/sec		
14		Unblocked	Online	F Port	2 Gb/sec		
15		Unblocked	Online	F Port	2 Gb/sec		
16		Unblocked	No Light	G Port	Not Established		

Figure 1–6: Port List View

The **Port List** view displays information about all ports installed in the Switch. All data is dynamic and updates automatically. Double-click any row in this view to display the **Port Properties** dialog box for the port.

Right-click a port row to display the same menu options that display when you right-click a port in the **Hardware** view or a port's bar graph in the **Performance** view. These include:

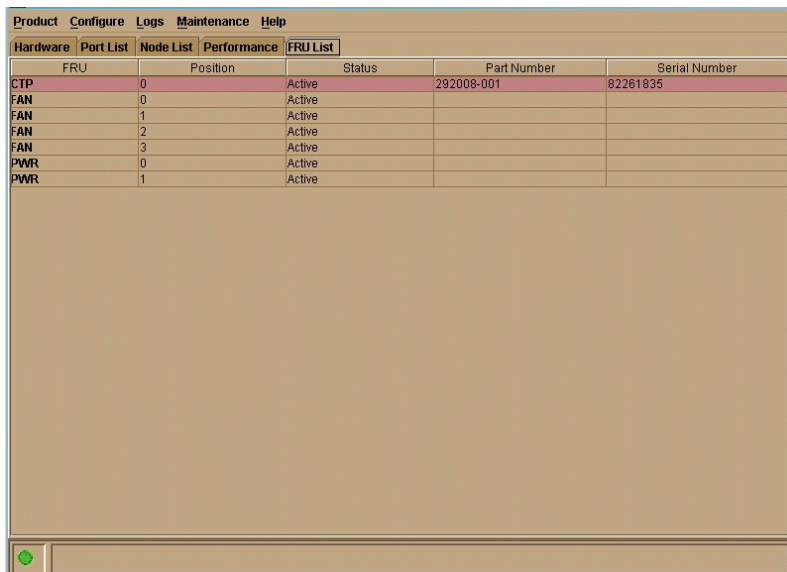
- Port Properties
- Node Properties
- Port Technology
- Block Port
- Enable Beaconing
- Port Diagnostics

- Channel Wrap (S/390 mode only)
- Swap Ports (S/390 mode only)
- Clear Link Incident Alert(s)
- Reset Port
- Port Binding
- Clear Threshold Alert(s)

Note that these options are also available when you click a port row and choose the **Port** secondary menu from the **Product** menu on the menu bar. For details on these menu options, refer to [Port Menu on page 2-16](#). For details on navigating and monitoring via the **Port List** view, refer to [Port List View on page 1-27](#).

FRU List View

Choose the **FRU List** view tab. A table with information about each of the FRUs installed in the Switch displays in the view panel. All data is dynamic and updates automatically. [Figure 1-7](#) shows an example of the **FRU List** view.



Product Configure Logs Maintenance Help				
Hardware Port List Node List Performance FRU List				
FRU	Position	Status	Part Number	Serial Number
CTP	0	Active	292008-001	82261835
FAN	0	Active		
FAN	1	Active		
FAN	2	Active		
FAN	3	Active		
PWR	0	Active		
PWR	1	Active		

Figure 1-7: FRU List View

For details on navigating and monitoring via the **FRU List** view, refer to [FRU List View on page 2-24](#).

Node List View

Choose **Node List** from view tabs. [Figure 1–8 on page 1-29](#) shows an example of the **Node List** view. This view displays a table with information about all node attachments or N_Ports that have logged into existing F_Ports on the Switch. Only N_Ports display in the **Node List** view after nodes have logged in to the fabric. The columns that display in the table include: port number where the node is attached, the port's address (S/390 mode only), node type, WWN of the attached node (device), and BB_Credit used by the attached node.

Double-click a port row to highlight it and display the **Node Properties** dialog box for that port. Right-click a port row to display the following menu options:

- **Node Properties** — Displays the **Node Properties** dialog box.
- **Port Properties** — Displays the **Port Properties** dialog box.
- **Define Nickname** — Displays the **Define Nickname** dialog box, where you can define a nickname for the attached device instead of using the 8-byte WWN.
- **Display options** — Allows you to display attached devices listed under the **Port WWN** column in the **Node List** view by the device's nickname configured through the **Define Nickname** menu option or the device's WWN.

Product Configure Logs Maintenance Help					
Hardware Port List Node List Performance FRU List					
Port #	Address	Port WWN	Unit Type	BB_Credit	
3	650713	HP-50:06:0B:00:00:10:AD:10	Unspecified	4	
6	650A13	HP-50:06:0B:00:00:01:35:A0	Unspecified	4	
8	650C13	Emulex-10:00:00:00:C9:21:84:FC	Unspecified	64	
9	650D13	Emulex-10:00:00:00:C9:21:84:7E	Unspecified	64	
11	650F13	QLogic-21:00:00:E0:8B:05:0A:62	Unspecified	3	
13	651113	QLogic-21:00:00:E0:8B:05:04:62	Unspecified	3	
14	651213	QLogic-21:00:00:E0:8B:05:13:62	Unspecified	3	
15	651313	QLogic-21:00:00:E0:8B:05:08:62	Unspecified	3	

Figure 1–8: Node List View

Note that these options are also available when you click a port row, then choose the **Port** secondary menu from the **Product** tab on the menu bar.

For details on navigating and monitoring via the **Node List** view, refer to [Node List View on page 1-29](#).

Performance View

Choose the **Performance** view tab. [Figure 1–9](#) shows an example of the **Performance** view. This view provides a graphical display of performance for all 32 ports. The top portion of the **Performance** view displays bar graphs that show the level of transmit/receive activity for each port. This information updates every five seconds. Each bar graph also shows the percentage link utilization for the port. A red arrow marks the highest utilization level reached since the **Performance** view was opened. If the system detects activity on a port, it shows minimal activity with at least one bar.

When an end device (node) is logged into a port, moving the cursor over the port's bar graph in the **Performance** view highlights the graph and displays a message with the World Wide Name of the connected node. If the connected node has more than one port, this is the World Wide Name of the specific port on the node. When a port is functioning as an expansion port (E_Port), the message is "E_Port." When a port is not logged into an end-device (not functioning as an F_Port) or to another Switch (not functioning as an E_Port), the message is the port's current online state.

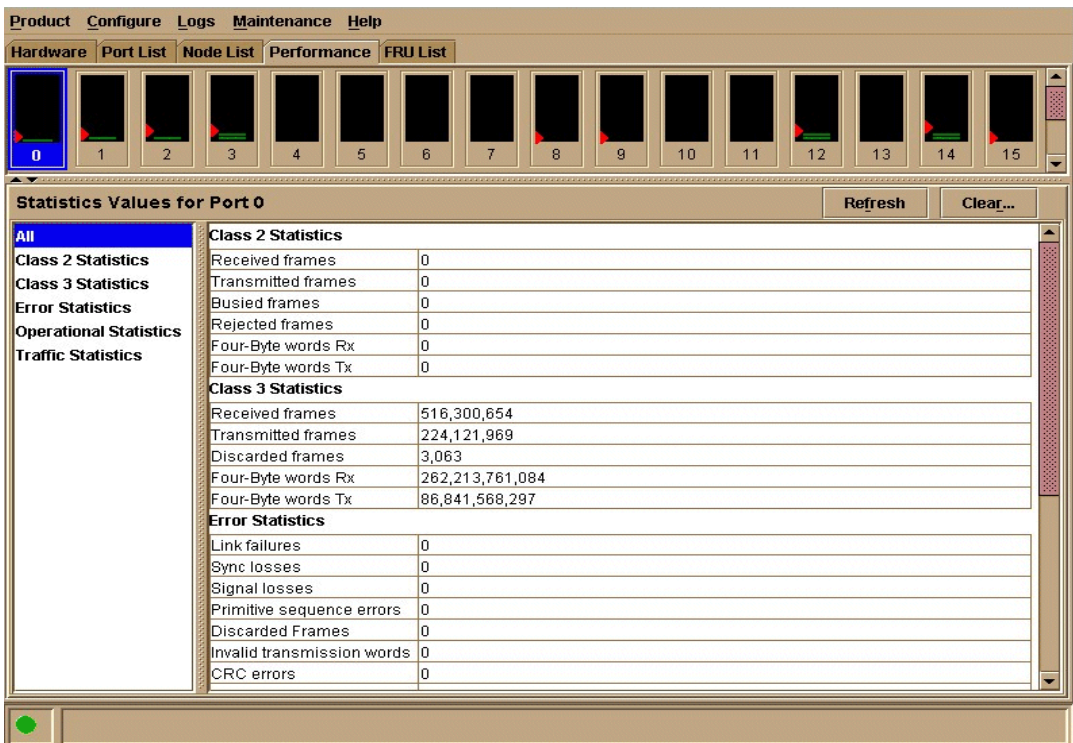


Figure 1–9: Performance View

Right-click a bar graph to display a menu of port-related actions. The options available on this menu are the same as those that are available when you right-click a port in the **Hardware** view or right-click a row in the **Port List** view. These include:

- Port Properties
- Node Properties
- Port Technology
- Block Port
- Enable Beaconing
- Port Diagnostics
- Channel Wrap (S/390 mode only)
- Swap Ports (S/390 mode only)
- Clear Link Incident Alert(s)
- Reset Port
- Port Binding
- Clear Threshold Alert(s)

Note that these same options are also available when you click a port's graph, then choose the **Port** secondary menu from the **Product** menu on the menu bar.

For details on menu options, refer to [Port Menu on page 2-16](#).

The bottom portion of the **Performance** view displays cumulative statistical information for the port selected in the bar graph. Values are displayed for transmit and receive traffic, class 2 and 3 statistics, operational statistics, and error categories. Click a category in the left frame of the statistics area to display only statistics in that category or click **All** to display values for all categories. Click the **Refresh** button to update the data with current data from the port.

Click the **Clear** button to clear all of the counters to zero. Choosing this button displays a **Clear Port Statistics** dialog box. Choose the appropriate radio button and click OK to clear all counters to zero on the selected port only or counters on all ports on the Director.

NOTE: Clearing the counters clears the statistics for all users.

For more information about the **Performance** view, including statistics descriptions, refer to [Performance View on page 2-30](#).

Status Bar

The status bar is located along the bottom of the **Product Manager** window. This includes a symbol that displays at the left side of the bar and messages that display in the panel to the right of the symbol. The symbol indicates the current operating status of the Switch and the messages display to provide more description of menu options as you move the cursor over the options under menu bar menus. Refer to [Table 1–1 on page 1-32](#) for the meaning of these status symbols and of the corresponding alert text that displays in the Edge-32 **Status** table at the top of the **Hardware** view in the view panel.

If a gray square displays in the status bar (no Ethernet connection), a reason for the status displays in the **Status** table at the top of the **Hardware** view. Refer to [No Link Status on page 2-3](#) for details.

Table 1–1: Operating Status — Status Bar and Switch Status





Symbol	Status Bar	Switch Status Table Text	Meaning
	Green Circle	Fully Operational	All components and installed ports are operational; no failures.
	Yellow Triangle	Redundant Failure	A redundant component has failed, such as a power supply, and the backup component has taken over operation.
		Minor Failure	<p>A failure occurred which has decreased the Switch operational ability. Normal switching operations are not affected.</p> <p>One or more ports failed, but at least one port is still operational.</p> <p>A fan has failed or is not rotating sufficiently.</p>

Table 1–1: Operating Status — Status Bar and Switch Status (Continued)

Symbol	Status Bar	Switch Status Table Text	Meaning
	Blinking Red and Yellow Diamond	NOT OPERATIONAL	<p>A critical failure prevents the Switch from performing fundamental switching operations.</p> <p>All fans failed. All installed ports failed. Both power supplies failed.</p>
	Gray Square	Never Connected Link Timeout Protocol Mismatch Duplicate Session Unknown Network Address Incorrect Product Type	<p>Switch status is unknown. This occurs if the Ethernet network connection between the HAFM server and the Switch cannot be established or if the CTP fails. Refer to No Link Status on page 2-3 for details on the status table text.</p>

Messages display to the right of the status symbol as you move the cursor over options under the menu bar menus. These messages provide additional details about tasks that you can perform through the menu option.

Closing the Product Manager

To close the Product Manager, use the following steps:

- To close the Product Manager, do one of the following:
 - Choose **Close** from the **Product** menu on the menu bar.
 - Click the **X** button at the top right corner of the **Product Manager** window.
 - Double-click the icon at the top left corner of the **Product Manager** window, or right-click the icon and choose **Close** from the menu that displays.

2. Choose **Logout** or **Exit** from the **Product** menu in the *HAFM* application.
 - If you choose **Logout**, the **StorageWorks ha-fabric manager Login** dialog box displays. You can now log in again using a user name and password. Log into a different HAFM server by choosing a different server from the **HAFM Server** box.
 - If you choose **Exit**, the **Product** view window closes.

User Rights

The HAFM system administrator can assign levels of access, or “User Rights,” to Product Manager users through the *HAFM* application.

NOTE: Note that the HAFM system administrator only has view rights while operating in a specific *Product Manager* application. Conversely, a Product Manager product administrator only has view rights while operating in the *HAFM* application.

Detailed instructions concerning the assignment of user rights for both the *HAFM* and *Product Manager* applications appear in Chapter 3 of the *hp StorageWorks ha-fabric manager user guide*.

There are five levels of access or “user rights” that can be assigned to specific users:

- System Administrator
- Product Administrator
- Operator
- Maintenance
- View

By default, all users have view rights, which allow viewing configurations but not the changing configurations. View rights cannot be removed.

User(s) with system administrator rights can make all control and configuration changes implemented through the *HAFM* application.

User Rights for Specific Functions

Table 1–2 itemizes the specific functions available to Product Manager users that have been assigned “user rights” of product administrator, operator, or maintenance. If a user does not have the right to perform a specific operation, a not-authorized error box displays when the operation is attempted.

Table 1–2: User rights for Product Manager functions

Product Manager Rights	Product Administrator	Operator	Maintenance
Backup/Restore Configuration	X	X	X
Block Port	X	X	X
Change Online State	X		X
Channel Wrap (S/390 mode only)	X		X
Clear Audit Log	X		
Clear Event Log			X
Clear Hardware Log	X		X
Clear LIN Alert	X	X	X
Clear LIN Log	X		
Clear System Error Light			X
Clear Threshold Alerts	X		
Configure Addresses - “Active” (S/390 mode only)	X	X	
Configure Addresses - “Stored” (S/390 mode only)	X		
Configure Date/Time	X	X	X
Configure Feature Key	X		
Configure Identification	X		
Configure Management Server	X		
Configure Switch Parameters	X		

Table 1–2: User rights for Product Manager functions (Continued)

Product Manager Rights	Product Administrator	Operator	Maintenance
Configure Fabric Parameters	X		
Configure Port Binding	X	X	
Configure Ports	X	X	
Configure SNMP	X		
Configure Switch Binding	X		
Configure Threshold Alerts	X		
Configure Zoning	X		
Data Collection			X
Date/Time Sync Configuration	X	X	X
Enable Call Home Notification	X		X
Enable E-Mail Notification	X		X
Enable Telnet	X		
Enable Web Server	X		
Export Configuration Report	X	X	X
IPL	X	X	X
Manage Firmware			X
Port Beaconsing	X	X	X
Port Diagnostics			X
Reset Configuration			X
Reset Statistics Counters (Performance View)	X	X	
Reset Port	X		X
Set Online State	X	X	X
Swap Ports (S/390 mode only)	X		X

Table 1–2: User rights for Product Manager functions (Continued)

Product Manager Rights	Product Administrator	Operator	Maintenance
Unit Beaconsing	X	X	X
View Event Log	X	X	X
View Firmware			X
View Hardware Log	X	X	X
View LIN Log	X	X	X
View SNMP	X		X

Backing Up and Restoring Product Manager Data

As long as a Zip® disk remains in the Zip drive of the HAFM server, critical information from both the *Product Manager* and *HAFM* applications automatically backs up to the Zip disk when the data directory contents change or when you reboot the HAFM server.

The application used for this function is Iomega *QuikSync*, a separate application installed on the HAFM server. QuikSync is configured to automatically mirror the contents of the *HafmData* directory to the Zip drive when the contents are changed or when you reboot the HAFM server. This directory contains all HAFM and Product Manager data, so it can be copied back to a newly restored HAFM server to fully recover the preferred operating environment.

The mirroring operation will only occur while a user is logged in to Windows on the HAFM server PC (independent of the HAFM login).

The data contained in the *HafmData* directory and mirrored to the Zip disk includes the following:

- All HAFM configuration including:
 - Product definitions
 - User names, encrypted passwords, and user rights.
 - Nicknames
 - Session options
 - HAFM SNMP configurations
 - E-mail configuration

- All log files (both HAFM log files and individual Product Manager log files).
- Zoning library (all zone sets and zone definitions).
- Firmware library.
- Call-home configuration (including phone numbers and dialing options).
- Configuration data saved to the *HafmData* directory through the **Backup & Restore Configuration** option on the Product Manager **Maintenance** menu.

The *QuikSync* application will not backup certain Windows configurations that need to be reconfigured on a newly restored HAFM server, including the following:

- Windows user names and passwords.
- TCP/IP network configuration (such as IP address, gateway address, and DNS names).

The *QuikSync* application will be included on the *HAFM* Applications CD. It automatically installs on the HAFM server during the HAFM server install process. A blank Zip disk is required for each HAFM server and is included with the HAFM server deliverables.

Restoring Data to the HAFM server

To restore data to the HAFM server, copy the: *HafmData* directory from the zip disk to: *C:\hafmdata*.

Using QuikSync

For information on using QuikSync, refer to the *hp StorageWorks ha-fabric manager user guide*

Monitoring and Managing the Switch

This chapter describes how to use the features available in the Product Manager view panel to monitor and manage Switch operation. These features include status indicators, menu options, and dialog boxes available through the **Hardware** view, **Port List** view, **FRU List** view, **Node List** view, and **Performance** view.

Hardware View

The **Hardware** view is the default view when you open the Product Manager. If another view displays, display the **Hardware** view by choosing **Hardware** from view tabs on the **Product Manager** window. Using this graphical view of the Switch, you can view status symbols and simulated light emitting diode (LED) indicators, display data, and use mouse functions to monitor status and obtain vital product information for the Switch and its hardware components.

Identifying FRUs

Move the cursor over parts of the Switch graphic in the **Hardware** view to display labels identifying each hardware component and its slot position in the chassis relative to identical components installed in the Switch. Components include:

- Fan module. The Edge Switch 2/32 contains four single-fan modules.
- Power supply module. Note that each AC connector on the rear of the unit is the location of an internal power supply.
- Ports (small form factor LC transceivers).

Monitoring Switch Operation

Monitor the operating status of the Switch using the Switch **Status** table on the **Hardware** view and the status indicator on the status bar at the bottom of the **Product Manager** window.

Switch Status Table

The **Status** table at the top of the **Hardware** view displays the Switch's operational status, operational state, name, description, and location.

Status

Refer to [Table 2-1 on page 2-36](#) for the meaning of the text that displays in the Switch **Status** table and the corresponding status symbols that display on the status bar.

State

The **Status** field displays one of the following:

- **OFFLINE** — When the Switch is “OFFLINE,” all ports are offline. The ports cannot accept a login from an attached device or cannot connect to other Switches. You can configure this state through the **Set Online State** dialog box. Refer to [Set Online State on page 5-4](#) for instructions.
- **Online** — All unblocked ports are able to connect with devices. You can configure this state through the **Set Online State** dialog box. Refer to [Set Online State on page 5-4](#) for instructions. Note that the Switch automatically goes online after a power-up, an initial machine load (IML), or initial program load (IPL).
- **Coming online** — This is a transitional state that occurs just before the Switch goes online. This state normally only happens briefly, unless there is a problem reaching the online state.
- **Going offline** — This is a transitional state that occurs just before the Switch goes offline. This state normally only happens briefly, unless there is a problem reaching the offline state.

No Link Status

If the Ethernet network connection between the HAFM server and the Switch is down, the **Hardware** view displays the front and rear of the unit without FRUs. The Switch **Status** table at the top of the **Hardware** view changes to display the status (No Link) and reason with a yellow background. The name, description, and location fields are blank.

The **Reason** field on the Switch **Status** table displays one of the following reasons when there are no links:

- **Never Connected** — A network connection was never established between the Switch and the HAFM server or if the CTP card has failed. Check the IP addresses, the Ethernet local area network (LAN) physical connection between the Switch and HAFM server, and other network connection conditions.

Note that the CTP card is not a FRU. If it fails, the Switch must be replaced.

- **Link Timeout** — The network connection that was established between the Switch and HAFM server has been lost. Check the IP addresses, the Ethernet LAN physical connection between the Switch and HAFM server, IP addresses, and other network components.
- **Protocol Mismatch** — The Switch and the HAFM server are not at compatible software release levels. Update the HAFM software version.
- **Duplicate Session** — A link has previously been established between the Switch and another instance of the HAFM server. Connect to the previously established HAFM server from the HAFM login screen.
- **Unknown Network Address** — The address defined for the Switch in the HAFM could not be found in the domain name server (DNS). Either the name was mistyped when the Switch was added to the HAFM, or the name was not available from the DNS. Check the network IP address for the Switch definition in the HAFM by right-clicking the product icon and choosing **Properties**. The IP address displays in the **Network Address** field.
- **Incorrect Product Type** — The product at the configured network address is not a Switch. Verify address, configuration, and product type.

Status Bar Status Indicator

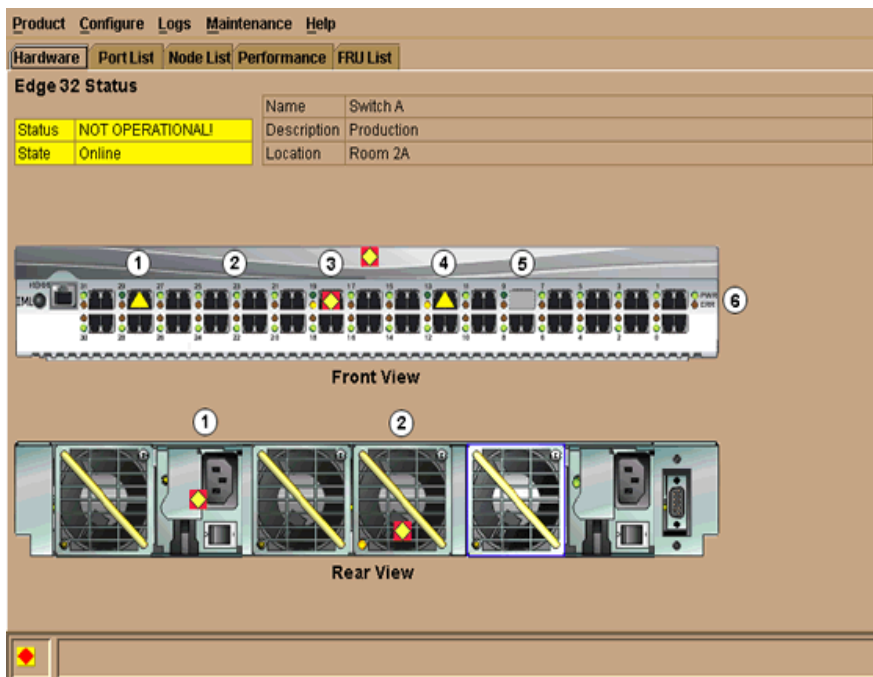
The status bar displays a colored status symbol that indicates the overall operating status of the Switch unit. The operating status depends on hardware component failures, which are indicated by status symbols that display over component graphics in the **Hardware** view. Refer to [Hardware View on page 2-1](#) for the meanings of status symbols in the status bar.

The status bar indicates the Switch operating status based on component failures. For example, for a single port failure, a blinking red and yellow diamond displays on the port connector in the **Hardware** view. At the same time, a yellow triangle displays in the status bar to indicate a degraded Switch. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a red and yellow diamond, indicating a failure that requires immediate attention.

Monitoring Hardware Operation

Determine hardware component operating status and states by the simulated light emitting diode (LED) indicators and status symbols, such as flashing red and yellow diamonds and yellow triangles, that display on hardware components. These simulated LEDs and status symbols reflect the state of the actual hardware as changes occur. Corresponding or additional descriptions of hardware status and states also display when you double-click components to display **Properties** dialog boxes.

[Figure 2-1](#) illustrates the **Hardware** view for the Edge Switch 2/32. The figure includes examples of symbols and LED indicators that display to help you monitor hardware operation. Numbers by each example are keyed to descriptions under [Front View](#) (following) and [Rear View on page 2-7](#).



- | | |
|----------------------------|---|
| ❶ Port Attention Indicator | ❷ Beacons or Diagnostic Test |
| ❸ Port LED Indicator | ❸ Not Installed |
| ❹ Port Failure Indicator | ❹ Power, System Error, and Unit Beacons |

Figure 2–1: Monitoring hardware operation — Edge Switch 2/32 Hardware view

Front View

1. **Port Attention Indicator** — The yellow triangle (▲) indicates that a link incident occurred or that the port is not operational, in nonstandard mode of operation, or has other status. For a link incident, the status table at the top of the **Hardware** view changes to reflect the reason for the alert. You can also note the reason by displaying the **Port Properties** dialog box for the port. For details on status indicators, refer to [Table 2–1 on page 2-36](#). For details on link incidents, refer to [Link Incident Alerts on page 2-39](#).

2. **Port LED Indicator** — A green and amber indicator to the left of each port connector simulates LED operation on the actual Switch port. When the green indicator illuminates, the port is online and operational. When the amber indicator illuminates steady, the port has failed. For details on port LED indicator operation, see [Table 2–1 on page 2-36](#).
3. **Port Failure Indicator** — A blinking red and yellow diamond (🔴🟡) below a port connector indicates that the port has failed. Refer to [Table 2–1 on page 2-36](#) for details on port operating states and the status symbol and indicator operation.
4. **Beaconing or Diagnostic Test** — When a blinking amber LED indicator displays by a port and an attention indicator (🟡) displays below the port's connector, either diagnostic tests are running on the port or beaconing is enabled. Refer to [Table 2–1 on page 2-36](#) for details on port operating states and the status symbol and indicator operation.
5. **Not Installed** — The port optics are not installed, or the feature that provides additional port function is not enabled.
6. **Power, System Error, and Unit Beaconing Indicators** — The green and amber indicators on the far right of the front view simulates the power and system error LEDs on the actual Switch.
 - **Power Indicator** — The green indicator (**PWR**) simulates the power LED on the actual Switch. When the indicator illuminates, the Switch is connected to facility AC power and is operational. The indicator will be on if either power supply is operating.
 - **System Error Indicator** — The amber system error light indicator (**ERR**) simulates the system error light on the actual Switch. When this indicator illuminates, an event has occurred requiring immediate attention, such as a system, fan, power supply, or port failure. View details of system errors by choosing **Event Log** from the **Logs** menu on the Product Manager menu bar. The indicator in the **Hardware** view and the LED on the actual unit remains illuminated until you clear the event by right-clicking on the front or rear view away from a hardware component and choosing **Clear System Error Light** from the menu.
 - **Unit Beaconing Indicator** — The amber indicator blinks if unit beaconing is enabled. Enable and disable unit beaconing by right-clicking on the front or rear view away from a hardware component and choosing **Enable Unit Beaconing** from the menu.

Rear View

1. **Power Supply Status** — Each AC power connector indicates the location of an internal power supply. A simulated green LED indicator is located in the upper left corner of each AC power connector. The indicator illuminates if the power supply is working and receiving AC power.

When a blinking red and yellow diamond (🔴🟡) displays on a power connector, like in [Figure 2–1 on page 2-5](#), the internal power supply for that connector failed. In this case, the green indicator to the top left of the connector will not illuminate. When the green indicator is on and no status symbol displays, the power supply is operational. Note that the Switch operates with one power supply failure, however replace the power supply as soon as possible to retain redundancy.

2. **Fan Status** — Four fan modules are installed in the Edge Switch 2/32 to cool the power supplies and CTP card. Note that the CTP card is an internal component and not a FRU.

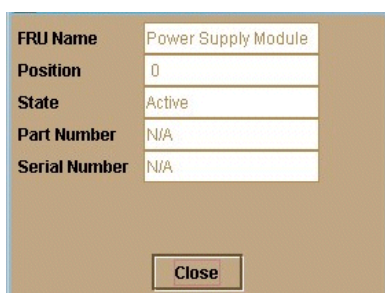
A simulated amber LED is located in the above left corner of each fan module. When the LED indicator on a fan module illuminates, as shown in the previous illustrations, and a blinking red and yellow diamond (🔴🟡) displays over a module, the fan has failed or is rotating insufficiently. You should replace failed fan modules as soon as possible. Note that the Switch continues to operate with one fan failure. If two or more fans fail, replace them as soon as possible to avoid Switch damage.

Obtaining Hardware Information

This section explains how to access the **FRU Properties**, **Port Properties**, and **Switch Properties** dialog boxes.

Displaying FRU Information

Double-click a fan or power supply (AC connector) in the **Hardware** view to display the **FRU Properties** dialog box. This dialog box displays the FRU name; slot position relative to identical FRUs installed in the chassis; active or failed state; part number; and serial number.

The image shows a dialog box titled "FRU Properties". It has a light brown background. On the left, there are five labels: "FRU Name", "Position", "State", "Part Number", and "Serial Number". To the right of each label is a text input field. The "FRU Name" field contains "Power Supply Module". The "Position" field contains "0". The "State" field contains "Active". The "Part Number" field contains "N/A". The "Serial Number" field contains "N/A". At the bottom center of the dialog box is a "Close" button.

FRU Name	Power Supply Module
Position	0
State	Active
Part Number	N/A
Serial Number	N/A

Close

Figure 2–2: FRU Properties dialog box

Displaying Port Information

Double-click a port or right-click a port and choose **Port Properties** from the menu to display the **Port Properties** dialog box (Figure 2–3). Also display this dialog box by:

- Double-clicking a row in the **Port List** view or right-clicking on a row and choosing **Port Properties** from the menu.
- Double-clicking a port's bar graph in the **Performance** view or right-clicking on the bar graph and choosing **Port Properties** from the menu.
- Right-clicking a port's row in the **Node List** view and choosing **Port Properties** from the menu
- Clicking a port, port row, or port bar graph in the preceding views and choosing the **Port** secondary menu from the **Product** menu on the menu bar.

Port Number	13
Port Name	
Type	F_Port
Operating Speed	1 Gb/sec
Fibre Channel Address	011113
Port WWN	McDATA-20:11:08:00:88:00:21:00
Attached Port WWN	Emulex-20:0D:00:00:C9:00:00:00
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	Online
Reason	
Threshold Alert	

Close

Figure 2–3: Port Properties dialog box

The following describes the fields in the port properties dialog box:

- **Port Number** — The physical port number.
- **Port Name** — User-defined port name or description. Refer to [Configure Ports on page 3–10](#) for instructions.
- **Type**
 - **G_port** — This displays if nothing is logged into the port.
 - **F_Port** — This displays if a device is logged into the port.
 - **E_Port** — This displays if the port is connected to another Switch's E_Port via an ISL.
- **Operating Speed** — This field displays the current data speed for the port as 1 Gb/sec, 2 Gb/sec, or Not Established. "Not Established" displays if Negotiate was set for the port through the **Configure Ports** dialog box and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating.
- **Fibre Channel Address** — The port's Fibre Channel address identifier.
- **Port WWN** — The port's 16-digit World Wide Name (WWN).

- **Attached Port WWN** — The WWN of the node logged into the port.
- **Block Configuration** — Blocked or unblocked. Operation can be blocked or unblocked through the **Configure Ports** dialog box. Refer to [Configure Ports on page 3–10](#) for instructions.
- **10-100 km Configuration** — Extended distance buffering. This can be enabled or disabled for the port through the **Configure Ports** dialog box. Refer to [Configure Ports on page 3–10](#) for instructions.
- **LIN Alerts Configuration** — This field indicates whether LIN alerts are enabled or disabled. LIN alerts can be configured through the **Configure Ports** dialog box. The default is for the LIN alerts to be enabled.
- **Beaconing** — This field indicates the beaconing status for the port. To enable or disable beaconing, right-click the port and choose **Enable Beaconing**.
- **Link Incident** — Description of the last link incident that occurred on the port.
- **Operational State** — Beaconing, inactive, invalid attachment, link incident, link reset, no light, not operational, online, offline, port failure, segmented E_Port, testing, or not installed. Refer to [Table 2–1 on page 2-36](#) for definitions of operational states.
- **Reason** — When the port operating state is “Segmented E_Port,” “Invalid Attachment,” or “Inactive,” this field displays the reason for that state. When an E_Port is segmented, two fabrics are prevented from joining. This only occurs when the Switch is connected to another Switch. Reasons and probable causes are listed under **Reason Field Messages** below.
- **Threshold Alert** — If a threshold alert exists for the port, an alert indicator (yellow triangle) displays by the **Threshold Alert** field, and the configured name for the last alert received displays in the field.

Reason Field Messages

The following messages display in the **Reason** field of the **Port Properties** dialog box if an Invalid Attachment, Segmented E_Port, or Inactive state occurs for the port.

Invalid Attachment Messages:

- **01 Unknown** — Invalid attachment reason cannot be determined.
- **02 ISL connection not allowed on this port** — Port is configured as an F_Port, but connected to Switch or Director.

- **03 ELP rejected by the attached switch** — This Director/Switch transmitted an exchange link protocol (ELP) frame that was rejected by the Switch at the other end of the ISL.
- **04 Incompatible switch at the other end of the ISL** — Interop mode for this Switch is set to Open Fabric mode and the Switch at the other end of the ISL is a HP Switch configured for Homogeneous Fabric mode.
- **05 External loopback adapter connected to the port.** — A loopback plug. is connected to the port and there is no diagnostic test running.
- **06 N_Port connection not allowed on this port** — The port type configuration does not match the actual port use. Port is configured as an E_Port, but attaches to a node device.
- **07 Non-HP switch at other end of the ISL** — The cable is connected to a non-HP Switch and interop mode is set to Homogeneous fabric mode.
- **08 ISL connection not allowed on this port** — The port type configuration does not match the actual port use (the port is configured as an F_Port, but attaches to a Switch or Director).
- **10 Port binding violation - unauthorized WWN** — The WWN entered to configure port binding is not valid or a nickname was used that is not configured through the Product Manager for the attached device.
- **11 Unresponsive node connected to port** — Possible causes are:
 - Hardware problem on Switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login in (FLOGI) cannot be received. There may be problems in Switch SBAR.
 - Faulty or dirty cable connection.
 - Faulty host bus adapters that do not send out FLOGI within reasonable timeframe.

Segmented E_Port Messages:

- **Incompatible operating parameters, such as resource allocation time-out values (R_A_TOV) or error-detect time-out values (E_D_TOV) are inconsistent.** Refer to [Configure Switch Operating Parameters on page 3–3](#) for more information.
- **Duplicate domain IDs.** Refer to [Domain ID on page 3–4](#) for more information.
- **Incompatible zoning configurations.** Refer to sections on joining zoned fabrics in the *hp StorageWorks edge switch 2/32 service manual* and the *hp StorageWorks ha-fabric manager user guide* for details.

- **Build fabric protocol error.**
- **No principal switch (no switch in the fabric is capable of being principal switch).**
- **No response from an attached switch.**

Inactive Messages:

Optics speed conflict. An inactive state will occur if you set the port's data speed to 2 Gb/sec for a 2 Gb/sec port module, and then replace the port module with a 1 Gb/sec module. To activate the port in this case, replace the module with a module that supports 2 Gb/sec data speed.

Displaying Switch Information

Double-click the Switch illustration, away from a hardware component, to display the **Switch Properties** dialog box as shown in the following figure.

Name	DracoLab-27
Description	Edge switch 2/32
Location	DracoLab
Contact	A. D. Ministrator, ext. 1234
World Wide Name	McDATA-10:00:08:00:88:A0:A2:8D
Type Number	003232
Model Number	001
Manufacturer	MCD
Serial Number	USM0T00011
EC Level	1YYMMDD
Firmware Level	04.01.00 8
Operating Mode	Open Systems
Preferred Domain ID	27
Active Domain ID	27
FC Address Domain	7B (hexadecimal)
CTP State	Active
Switch Speed	2 Gb/sec
Switch Binding	Disabled
<input type="button" value="Close"/>	

Figure 2–4: Switch Properties dialog box

The following displays in this dialog box:

- Switch name, description, location, and contact configured through the **Configure Identification** dialog box
- Fibre Channel World Wide Name (WWN) identifier for the Switch
- Product type number

- Product model number
- Product manufacturer
- Product serial number
- Engineering change (EC) level
- Firmware level
- Operating Mode
- Preferred Domain ID — This is set through the **Configure Operating Parameters** dialog box
- Active Domain ID — The actual domain ID assigned to the Switch
- Switch Speed — This is always 2 Gb/sec
- FC Address DomainID — Hexadecimal value indicating FC address domain
- CTP StateID — Active or Inactive
- Switch Binding — Enabled if the optional SANtegrity features are installed and enabled; otherwise, disabled displays

Using Menu Options

Right-click various parts of the **Hardware** view to display menu options for displaying status and information and for controlling the Switch and various hardware components.

Switch Menu

Right-click any area of the Switch illustration where a FRU hardware component is not installed to display the following menu options.

Switch Properties

Click to display the **Switch Properties** dialog box. This dialog box contains the Switch name, description, location, and contact person configured through the **Configure Identification** dialog box. Also included is other product information as detailed in [Displaying Switch Information on page 2-12](#). You can also display this dialog box by double-clicking an area on the illustration away from a hardware component.

Enable Unit Beaconing

Click the check box to toggle unit beaconing on or off. When the check box has a check mark, unit beaconing is on, and the system error light (**ERR**) on the Switch blinks to help users locate the unit managed by the Product Manager. The amber indicator on the **Hardware** view also blinks when beaconing is enabled. When you click the check box to remove the check mark, the unit beaconing is disabled.

NOTE: You can only enable beaconing if there are no system errors (the system error light is off).

Clear System Error Light

Choose this option to turn off the amber system error light (**ERR**), located below the green power (**PWR**) LED on the Switch. This also turns off the amber system error light indicator in the **Hardware** view (front view)

IPL Switch

Choose this option to initiate an IPL on the Switch. When the dialog box displays confirming the IPL, click **Yes**.

NOTE: An IPL is not intended for ordinary or casual use and should only be performed when directed by your support personnel.

Refer to [Execute an IPL on page 5–3](#) for detailed procedures.

Set Switch Date and Time

Choose this option to display the **Configure Date and Time** dialog box.

1. Click to display the **Configure Date and Time** dialog box.

The dialog box displays with a check mark (the default) in the **Periodic Date/Time Synchronization** check box. If this field is checked, the HAFM server periodically sets the Switch time to automatically synchronize with the HAFM server time. Daylight savings time automatically updates on the Switch using this option.

The current date and time display in the **Date** and **Time** fields. If the **Periodic Date/Time Synchronization** field is checked, the **Date** and **Time** fields are disabled (grayed out).

To enable and disable **Periodic Date/Time Synchronization**, select the check box and then click **Activate**.

Figure 2–5: Configure Date and Time Periodic Synchronization dialog box

2. Perform one of the following steps:

- To immediately synchronize the Switch date and time with the HAFM server, be sure the **Periodic Date/Time Synchronization** option is enabled and then click **Sync Now**.

NOTE: If you enable the **Periodic Date/Time Synchronization** feature and click **Activate**, the time will synchronize at the next update period.

- To set the Switch with a specific date and time, make sure that the **Periodic Date/Time Synchronization** field is not selected. Refer to [Figure 2–6](#). Enter the date and time and then click **Activate**.
- S/390 mode only. An error will result if periodic synchronization and Switch clock alert mode are enabled (refer to [Configuring the FICON Management Server on page 6–2](#)). Note that this error would not occur if the FICON Management Server feature is enabled on the Switch.

Figure 2–6: Configure date and time manually

NOTE: Use the range of 0 to 23 for hours. Use the range of 0 to 59 for minutes and seconds.

Set Switch Online State

Click to display the **Set Online State** dialog box. The dialog box displays the current state (offline or online) and provides a button for changing the state.



CAUTION: Before setting the Switch offline, warn administrators and users currently operating attached devices that the Switch is going offline and that there will be a disruption of port operation. Also, request that the devices affected by an interruption of data flow be set offline.

1. Click the **Set Offline** or **Set Online** button to toggle between the states.

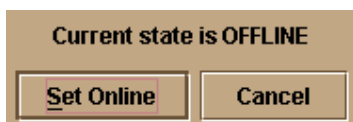


Figure 2-7: Set Online State dialog box (Offline)

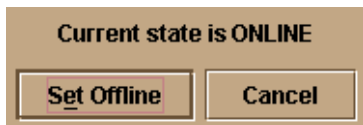


Figure 2-8: Set Online State dialog box (Online)

2. When the **Set Online** or **Set Offline** warning dialog box displays, click **OK** to set the Switch online or offline.

As the Switch goes offline, the word, “OFFLINE,” displays in the **State** field in the left corner of the **Hardware** view. As the Switch goes online, the word, “ONLINE,” displays in the **State** field in the left corner of the **Hardware** view. When going offline, LED indicators on all ports with attached devices stay green, but the Switch sends offline sequences (OLS) to these devices.

Port Menu

While in the **Hardware** view, right-click any port to display the following menu options.

Port Properties

Click this to display the **Port Properties** dialog box. This dialog box displays technical information about the port. See [Displaying Port Information on page 2-8](#) for more information.

Node Properties

Click this to display the **Node Properties** dialog box. Note that if a node is not logged into the port, a message displays indicating that node information is not available. For details on information that displays in this dialog box, refer to [Displaying Node Properties on page 2-28](#).

Port Technology


Click this to display the **Port Technology** dialog box. This dialog box displays the following information:

- Port number.
- Connector type: Always LC.
- Transceiver type: Longwave laser LC or shortwave laser LC.
- Distance: General distance range for port transmission. This can be either short to long distances for the longwave laser LC transceiver or short distances for the shortwave laser LC transceivers.
- Media: The Fibre Channel mode and optic size. For the longwave laser LC transceiver, this would be singlemode 9-micron. For the shortwave laser LC transceiver, this would be multimode 50-micron or 62.5-micron.
- Speed: This will be either 1 Gbit per second or 1 Gbit, 2 Gbit per second.

Block Port

Click to display a check mark and block port transmission. If blocked, a node attached to the port is prevented from logging into the Switch or communicating with other devices attached to Switch ports. A blocked port continuously transmits offline signals (OLS). Click to remove the check mark and unblock the port. If unblocked, a node attached to the port can communicate with the Switch and communicate with other nodes attached to the Switch.

Enable Beaconing

Click this to make the amber LED by the port blink on the actual Switch and the amber indicator blink for the port in the **Hardware** view. This enables users to locate the unit where the port is located. When a blinking amber LED indicator displays by a port, an attention indicator () displays below the port's connector in the **Hardware** view and in the port's row in the **Port List** view.

Port Diagnostics

Click this option to display the **Port Diagnostics** dialog box. Use this dialog box to run an internal loopback and external loopback test on the port. The **Port Diagnostics** option enables you to run internal and external loopback tests on any port. To use this option, follow the detailed steps in the *hp StorageWorks edge switch 2/32 service manual*.

Channel Wrap (S/390 mode only)

Click this while in S/390 mode to display a check mark and allow a channel wrap test to be initiated from an attached host or device. In this test, frames are sent to the Switch port, then the Switch echoes the frames back to the sending device to test the channel. The Switch remains in channel wrap mode until the option is disabled. While in channel wrap mode, the port can only accept echo commands from the host and will appear to be blocked to all other communication. Click the check box to remove the check mark and disable channel wrap.

Swap Ports (S/390 mode only)

Click this while in S/390 mode to display the **Swap Ports** dialog box. Use this dialog box to swap addresses between ports. For details, refer to [Swap Ports on page 5–1](#).

Clear Link Incident Alert(s)

Click this to clear the attention indicator on the **Hardware** view, the **Port List** view, and the **Performance** view. In addition, the procedure clears the alert description in **Port Properties** dialog boxes. If there are no link incident alerts set for a port, no actions occur. Although you can manually clear link incidents, they may also be cleared by actions outside of the user interface, such as when rebooting the HAFM server.

Reset Port

Click to display a confirmation dialog box. Click **Yes** on that dialog box to reset the port. If a Switch is attached to the port and online, this operation sends a link reset to the attached Switch, otherwise this action disables port beaconing for the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state, clearing the service required (amber) LED. The reset does not affect other ports in the Switch.

Port Binding

Click to display the **Bind WWN** dialog box (Figure 2–9). Use this dialog box to allow a device with a specific WWN or nickname to have exclusive connection to a port. To use this dialog box, refer to the following paragraphs.

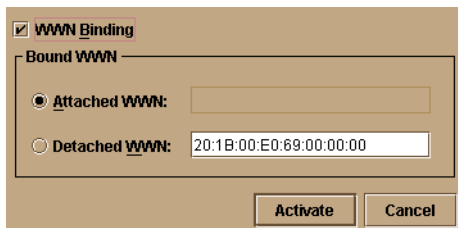


Figure 2–9: Bind WWN dialog box

Bind WWN dialog box parameters:

- **Port Binding** — Click this check box to place check mark in the box and enable WWN binding for the port. When enabled, only a specific device can communicate through the port. This device is specified by the WWN or nickname entered into the **Bound WWN** area (either the **Attached WWN** or **WWN** fields). With the check box cleared, any device can communicate through the port even if a WWN or nickname is specified in the **Bound WWN** field.
- **Attached WWN** — Click the radio button and, if a device is logged into the port, the device's WWN will display in the field. The device with this WWN or nickname will have exclusive communication privileges through the port if **Port Binding** is enabled.

NOTE: If you click this radio button to bind the port to a logged-in device and there are no devices logged in, the port is essentially bound to a WWN of "0." This prevents any device from logging in until this button is re-enabled to bind the WWN of a logged-in device or until you explicitly bind the WWN of a device by clicking the Detached WWN radio button and entering a WWN or nickname (see the following). Changes only take effect when you click the **Activate** button.

- **Detached WWN** — Click the button and enter a World Wide Name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through the Product or HAFM applications. The device with this WWN or nickname will have exclusive communication privileges through the port if **Port Binding** is enabled.

Note the following:

- If you do not enter valid WWN or nickname in this field, but the **Port Binding** check box is checked (enabled), then no devices can communicate through the port.
 - If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can communicate through the port.
- **Activate** — Click this button to activate settings in this dialog box.

Warning and error message display:

- If one or more of the nodes logged into to the port does not match the WWN or nickname configured in the field by the **WWN** radio button, a warning dialog box displays after you activate the configuration. This warning box displays a list of all nodes that will be logged off if you continue. If you click **Continue** on the warning box, these nodes will be logged off and the port can only communicate with the device with the WWN or nickname configured in the **WWN** field.
- An error message displays after you activate the configuration if the format for the WWN entered in the **WWN** field is not valid (not in xx.xx.xx.xx.xx.xx.xx.xx format) or if you have entered a nickname that was not configured through the Product Manager.

Clear Threshold Alert(s)

Click this to display the **Clear Threshold Alert(s)** dialog box. Choose the appropriate option to clear alerts for the selected port only or all ports on the Switch. This clears all attention indicators that notify users of threshold alerts in dialog boxes and views. This action also restarts the notification interval and the cumulative minutes for utilization % interval.

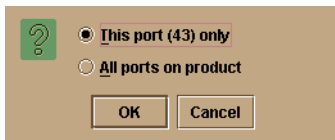


Figure 2–10: Clear Threshold Alert(s) dialog box

Port List View

Display the **Port List** view (Figure 2–11) in the view panel by choosing **Port List** from view tabs on the **Product Manager** window.

Product Configure Logs Maintenance Help							
Hardware Port List Node List Performance FRU List							
#	Name	Block Config	State	Type	Operating Speed	Alert	
0		Unblocked	Online	E Port	2 Gb/sec		
1		Unblocked	Online	E Port	2 Gb/sec		
2		Unblocked	No Light	F Port	1 Gb/sec		
3		Unblocked	Online	F Port	2 Gb/sec		
4		Unblocked	No Light	G Port	Not Established		
5		Unblocked	No Light	G Port	Not Established		
6		Unblocked	Online	F Port	1 Gb/sec		
7		Unblocked	No Light	G Port	Not Established		
8		Unblocked	Online	F Port	1 Gb/sec		
9		Unblocked	Online	F Port	1 Gb/sec		
10		Unblocked	No Light	G Port	Not Established		
11		Unblocked	Online	F Port	2 Gb/sec		
12		Unblocked	No Light	G Port	Not Established		
13		Unblocked	Online	F Port	2 Gb/sec		
14		Unblocked	Online	F Port	2 Gb/sec		
15		Unblocked	Online	F Port	2 Gb/sec		
16		Unblocked	No Light	G Port	Not Established		

Figure 2–11: Port List View

The **Port List** view displays the following information on all ports that can be installed in the Switch. All information is updated automatically.

- **#** — Number of the port from 0 through 31.
- **Addr** (S/390 mode only)

NOTE: This column only applies to S/390 mode and does not display during Open Systems mode.

Displays the logical address of the port. The logical address equals the port number, plus 4. For example, the address for port 0 is 4 (0+4). If port addresses have been swapped, those addresses will be followed by an asterisk (*).

- **Name** — Displays the port name as configured through the **Configure Ports** dialog box.
- **Block Config** — Indicates the blocked or unblocked configuration of the port as set through:
 - The **Configure Ports** dialog box.
 - The **Configure Addresses - “Active”** dialog box. (S/390 mode only).

The **Block Port** option available through the port right-click menu in the **Hardware** view, port row right-click menus in the **Port List** view, is also the port bar graph right-click menus in the **Performance view**, and the **Port** secondary menu of the **Product** menu on the menu bar.

Blocked states are:

- **Blocked** — Devices communicating with the port are prevented from logging into the Switch or communicating with other devices attached to Switch ports. A blocked port continuously transmits OLS.
- **Unblocked** — Devices communicating with the port can log in to the Switch and communicate with devices attached to any other unblocked port in the same zone.
- **State** — The following port operational states may display in this table. For more information on these states and corresponding status symbol and LED indicator operations in the Hardware view, see [Port Operational States on page 2-36](#).
 - No Light
 - Online
 - Offline
 - Beaconsing
 - Link Reset
 - Not Operational
 - Not Installed
 - Invalid Attachment
 - Port Failure
 - Segmented E_Port
 - Link Incident
 - Testing
 - Inactive

- **Type** — The type of port.
 - It is an F_Port if an N_Port is attached.
 - It is an E_Port if another E_Port is attached.
 - It is a G_Port if the port is capable of acting as either an F_Port or an E_Port, but nothing is currently attached.
- **Operating Speed** — This field displays the current data speed for the ports as 1 Gb/sec or 2 Gb/sec or Not Established.
- **Alert** — This column displays a yellow triangle if a link incident occurs on the port or if the port's LED is beaconing. Blinking red and yellow diamonds display for port failures or for ports requiring service. Click the row to display the reason for the alert in the **Port Properties** dialog box.

Double-click a row to display the **Port Properties** dialog box. For an explanation of the fields on the **Port Properties** dialog box, refer to [Displaying Port Information on page 2-8](#).

Menu Options

Right-click a row to select it, highlight it, and display a menu with the following port-related action options. These are the same menu options that display when you right-click a port in the **Hardware** view and port bar graph in the **Performance** view. You can also display this menu by clicking on a port, port row, or port bar graph in the preceding views and choosing the **Port** secondary menu from the **Product** menu on the menu bar.

Refer to [Port Menu on page 2-16](#) for details on these menu options.

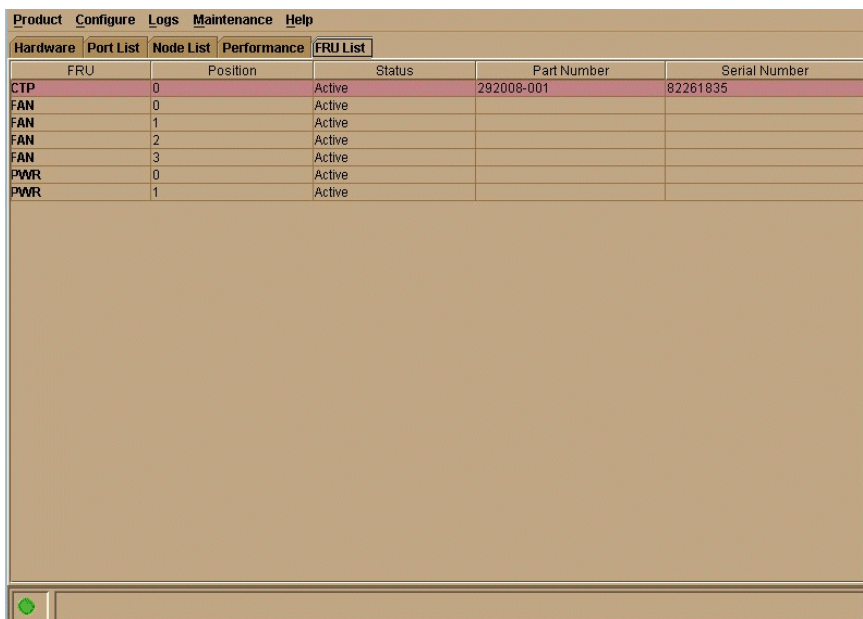
- Port Properties
- Node Properties
- Port Technology
- Block Port
- Enable Beaconing
- Port Diagnostics
- Channel Wrap (S/390 mode only)
- Swap ports (S/390 mode only)
- Clear Link Incident Alert

- Reset Port
- Port Binding
- Clear Threshold Alert(s)

NOTE: For **Node Properties**, if a node is not logged in a message displays indicating that node information is not available.

FRU List View

Display the **FRU List** view ([Figure 2–12 on page 2-24](#)) by choosing the **FRU List** view tab on the **Product Manager** window. This view displays information about all installed FRUs on the Switch. All data is dynamic and updates automatically as the software detects changes.



Product Configure Logs Maintenance Help				
Hardware Port List Node List Performance FRU List				
FRU	Position	Status	Part Number	Serial Number
CTP	0	Active	292008-001	82261835
FAN	0	Active		
FAN	1	Active		
FAN	2	Active		
FAN	3	Active		
PWR	0	Active		
PWR	1	Active		

Figure 2–12: FRU List View

Information on the **FRU List** view for each FRU includes:

- **FRU Name** — CTP (Control Processor) card, FAN (fan module), and PWR (power-supply module). Note that the CTP card is an internal component and is not a FRU. If it fails completely the entire Switch must be replaced.

- **Position** — Slot position of FRU in the chassis relative to identical FRUs also installed in the chassis.

There are four fan modules (positions 0-3), one CTP card (position 0), two power supplies (positions 0-1), and 32 port positions (0-31).

- **Status** — Active or failed. **Active** displays always unless the FRU fails. **Failed** displays if the FRU is not functional.
- **Part Number** — Part number of the FRU.
- **Serial Number** — Serial number of the FRU.

Node List View

Display the **Node List** view in the view panel by choosing **Node List** from the view tabs on the **Product Manager** window. This view displays information about all node attachments to any F_Ports on the Switch sorted by port number. All data is dynamic and updates automatically as devices log in and log out.

Product Configure Logs Maintenance Help					
Hardware	Port List	Node List	Performance	FRU List	
Port #	Address		Port WWN		Unit Type
3	650713		HP-50:06:0B:00:00:10:AD:10	Unspecified	4
6	650A13		HP-50:06:0B:00:00:01:35:A0	Unspecified	4
8	650C13		Emulex-10:00:00:00:C9:21:84:FC	Unspecified	64
9	650D13		Emulex-10:00:00:00:C9:21:84:7E	Unspecified	64
11	650F13		QLogic-21:00:00:E0:8B:05:0A:62	Unspecified	3
13	651113		QLogic-21:00:00:E0:8B:05:04:62	Unspecified	3
14	651213		QLogic-21:00:00:E0:8B:05:13:62	Unspecified	3
15	651313		QLogic-21:00:00:E0:8B:05:08:62	Unspecified	3

Figure 2–13: Node List View

Information that displays for each node includes:

- **Port #** — Number of the port, from 0 through 31.
- **Address**
 - In S/390 mode, this displays the logical port address (port number plus 4).
 - In Open Systems mode, this displays the node's Fibre Channel address.

- **Port WWN** — The port WWN of the attached node (N_Port). The 16-digit WWN is a set of unique numbers assigned to the device attached to the port. The WWN is prefixed by the manufacturer's name of the host bus adapter that attaches to the device. If there is a nickname assigned, the nickname displays instead of the WWN.
- **Unit Type** — The following information, if supported, is supplied by the attached device:
 - Unknown
 - Other
 - Hub
 - Switch
 - Gateway
 - Converter
 - HBA
 - Proxy-agent
 - Storage device
 - Host
 - Storage subsystem
 - Module
 - Software driver
 - Unspecified
 - Direct access storage
 - Magnetic tape
 - Unit record (input)
 - Unit record (output)
 - Printer
 - Communications controller
 - Terminal (full screen)
 - Terminal (line mode)
 - Stand-alone CTC adapter

- Switch
- Channel path ##
where ## will be replaced with the Channel Path Identifier (2 hex digits)
- Integrated CTC adapter
- Reserved
- **BB_Credit** — The buffer-to-buffer credit that the attached node has available.

Double-click a row to display the **Node Properties** dialog box. For an explanation of the fields on the **Node Properties** dialog box, refer to [Displaying Node Properties on page 2-28](#).

Menu Options

Right-click a row to select it, highlight it, and display a menu with the following port-related action options:

- **Node Properties** — Choose this option to display the **Node Properties** dialog box. Refer to [Displaying Node Properties on page 2-28](#).
- **Port Properties** — Choose this option to display the **Port Properties** dialog box (refer to [Figure 2-3 on page 2-9](#)).
- **Define Nickname** — Choose this option to display the **Define Nickname** dialog box, where you can define a nickname to display for the attached device instead of the device's 8-byte WWN.

The **Define Nickname** dialog box displays the World Wide Name (WWN) of the device attached to the port. To define a nickname, enter a name of up to 32 characters in the **Nickname** field and click **OK**. The nickname will display under the **Port WWN** column instead of the device's WWN.

- **Display Options** — Choose **Nickname** or **Worldwide Name** from the submenu. Choosing **Nickname** displays attached devices in the **Port WWN** column by the nickname configured through the **Define Nickname** menu option. Choosing **Worldwide Name** displays attached devices in the **Port WWN** column by the device's WWN.

Note that you can also display these menu options by clicking a port row, and choosing the **Port** secondary menu from the **Product** menu on the **Product Manager** menu bar.

Displaying Node Properties

Open the **Node Properties** dialog box by double-clicking a row in the **Node List** view or right-clicking a row and choosing **Node Properties** from the menu. You can also display this dialog box by right-clicking on a port in the **Hardware** view, right-clicking on a port's row in the **Port List** view, or right-clicking on a port's bar graph in the **Performance** view and choosing **Node List** from the menu that displays. In addition, you can display this dialog box by clicking to choose a port, port row, or port bar graph in the preceding views and choosing **Node Properties** from the **Port** secondary menu on the **Product** menu of the menu bar.

NOTE: If a node is not logged in, a message displays indicating that node information is not available.

Port Number	8
Fibre Channel Address	010C13
Port WWN	Emulex-20:08:00:00:C9:00:00:00
Port Nickname	
Node WWN	Emulex-20:08:00:00:C9:00:01:00
Node Nickname	
Unit Type	Reserved
Node Port Number	0
Buffer to Buffer Credit	4
Class of Service	Class 2
Data Field Size	10
<input type="button" value="Close"/>	

Figure 2-14: Node Properties dialog box

- **Port Number** — The physical port number on the Switch to which the node is connected.
- **Fibre Channel Address** — In Open Systems mode only, this displays the three-byte Fibre Channel Address of the mode.
- **Port Address** — In S/390 mode only, this field displays the logical address (port number plus 4) for the port where the node is attached.

NOTE: This field only applies during S/390 mode and does not display in Open Systems mode.

- **Port WWN** — Port World Wide Name of the attached device.
- **Port Nickname** — Nickname for the port WWN. Must be configured to display.

- **Node WWN** — Node World Wide Name of the attached device.
- **Node Nickname** — Nickname for the node WWN. Must be configured to display.
- **Unit Type** — Refer to Unit Type under [Node List View on page 2–25](#) for details.
- **Node Port Number** — The physical port number field of the node port that is attached to the Switch port (SB2- nodes only).
- **Buffer-to-Buffer Credit** — The buffer-to-buffer credit that the attached node has available.
- **Class of Service** — Class of service. This can be class 2, class 3, or both.
- **Data Field Size** — Data field size. This is the largest size of Fibre Channel frame the node will process. The size is negotiated with the attached device.

If the device is an SB-2 (FICON) node, additional information is displayed in the following fields:

- **Type** — The type number.
- **Model** — The model number.
- **Serial #** — Plant of manufacture and sequence number field.
- **Tag** — Tag field.

NOTE: Node Properties is also available from the menu that displays when you right-click a port's row in the **Port List** view or on a port's bar graph in the **Performance** view.

Performance View

Display the **Performance** view in the view panel by choosing **Performance** from the view tabs in the **Product Manager** window. This view displays a bar graph at the top of the view for each port. The lower portion of the view displays statistical values for the specific port's bar graph that you select.

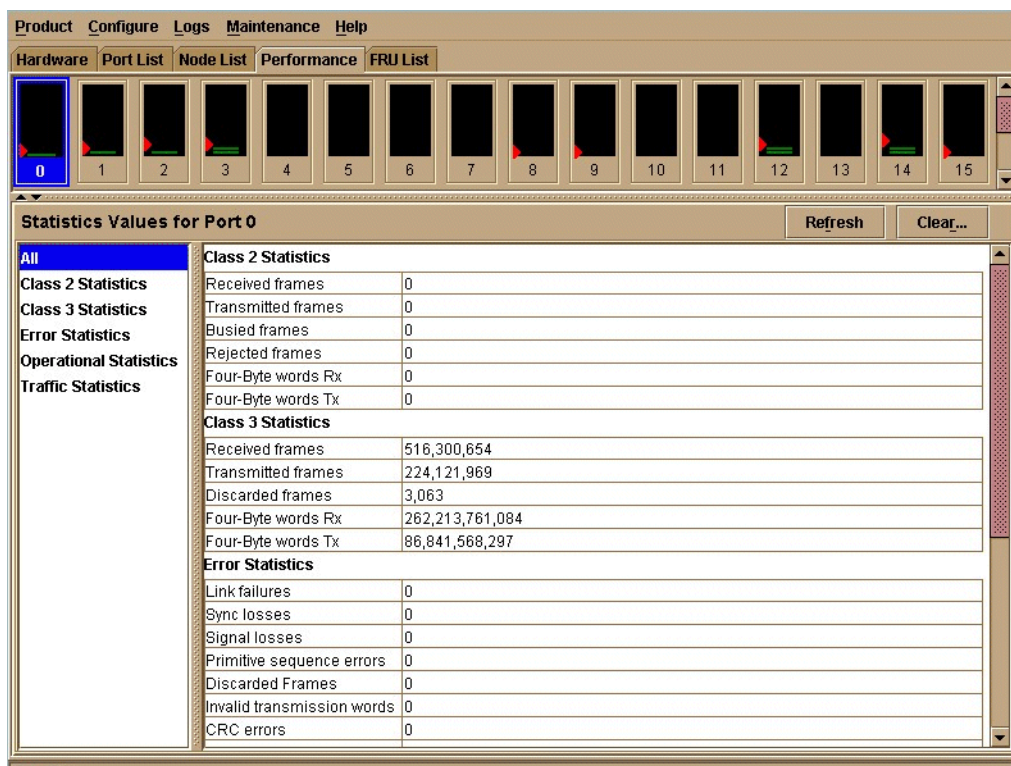


Figure 2–15: Performance view

Menu Options

Right-click any of the port bar graphs to display a menu with the following port-related action options. These are the same menu options that display when you right-click a port in the **Hardware** view or a port row in the **Port List** view. You can also display these options by clicking a port, port row, or port bar graph in the preceding views and choosing the **Port** secondary menu from the **Product** menu on the menu bar.

Refer to [Port Menu on page 2-16](#) for an explanation of these menu options.

- Port Properties
- Node Properties
- Port Technology
- Block Port
- Enable Beaconing
- Port Diagnostics
- Channel Wrap (S/390 mode only)
- Swap Ports (S/390 mode only)
- Clear Link Incident Alert(s)
- Reset Port
- Port Binding
- Clear Threshold Alert(s)

NOTE: For **Node Properties**, if a node is not logged in a message displays indicating that node information is not available.

Bar Graph Display

The **Performance** view provides a graphical display of performance for all ports. Each bar graph in the upper portion of the view panel displays the percentage of link utilization for the port. This information updates every five seconds. A red arrow marks the highest utilization since the opening of the **Performance** view. If the system detects activity on a port, it represents minimal activity with one bar.

When a port is logged in, moving the cursor over its bar graph displays a message with the attached port's WWN. If the port is an E_Port, the message reads, "E_Port" and if the port is not logged in, the message displays the port's current operational state (refer to [Table 2-1 on page 2-36](#)).

Port Statistics

To select and display more detailed performance information for a port, click the port's bar graph. The bar graph for that port highlights with a darker background and the lower portion of the **Performance** view panel displays the statistics values for the port's number and the WWN decoding.

The **Statistics Values** tables contain cumulative port statistics and error statistics for transmit and receive traffic, class 2 and 3 statistics, operational statistics, and error categories. Click a category in the left frame of the statistics area to display only statistics for that category or click All to display values for all categories.

For a description of the **Refresh** and **Clear** buttons, refer to [Button Functions on page 2-36](#).

Statistics Description

The **Statistics Values** tables contain statistics in the following groups. To refresh tables with the latest data, click the **Refresh** button on the upper right portion of the **Statistics Values** panel or click the port's bar graph. Clear all counters for all users using the **Clear** button.

Traffic Statistics with Receive and Transmit Values

This section describes the types of statistics that display when you click a port's bar graph:

- **Link utilization %** — There is a separate value for transmit and receive link utilization. The larger of these two values displays on the bar graph.

The current link utilization for the port is expressed as a percentage. Each port can transmit or receive data at 200 Megabytes (MB) per second. This statistic shows the percentage of the maximum link utilization currently being used. Link utilization is calculated over one-second intervals. The maximum link utilization is 100%.
- **Frames** — The number of frames that the port has received or transmitted.
- **Transmitted Frames** — The number of Class 2 frames transmitted by the F-Port to its attached N_Port.
- **Four byte words** — The number of words that the port has received or transmitted.
- **Offline sequences** — The number of offline sequence that the port has received or transmitted.

- **Link resets** — The number of link reset protocol frames received/transmitted by this port from/to the attached Switch. The Switch transmits a link reset to initiate the link reset protocol or recover from a link timeout. This occurs normally to establish BB_Credit or on any port in order to recover lost BB_Credit. The Switch receives a link reset from an attached device if the device wishes to initiate the link reset or recover from a link timeout.

There are not thresholds for these values. You may determine that a problem exists by the rate that the value changes. BB_Credit starvation can occur if data is sent to a device faster than it can consume the frames. This can backup into ISLs causing degraded performance.

Class 2 Statistics

The **Class 2 Statistics** table includes:

- **Received Frames** — The number of Class 2 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames** — The number of Class 2 frames transmitted by the F-Port to its attached N_Port.
- **Busied Frames** — The number of F_BSY frames generated by this F_Port against Class 2 frames. This can occur if frames are received before the Switch completes initialization or if the Switch is servicing so many requests that it can not process a new request. The port generates frames if the Switch is not ready to accept commands. This may indicate temporary congestion.
- **Rejected Frames** — The number of F_RJT frames generated by this F_Port against Class 2 frames.

These frames usually occur because of attached device errors. The device is expected to correct the error based on the reject code, then retry its request. If the device is able to recover, there is no cause for concern. If not, further troubleshooting may be necessary. There are no thresholds for this value. Typically, this occurs because the destination is not available due to the device's action.

- **Four Byte Words Received** — The number of four-byte words received.
- **Four Byte Words Transmitted** — The number of four-byte words transmitted.

Class 3 Statistics

The **Class 3 Statistics** table includes:

- **Received Frames** — The number of Class 3 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames** — The number of Class 3 frames transmitted by the F-Port to its attached N_Port.
- **Discarded Frames** — The number of Class 3 frames discarded, including multicast frames with bad D_IDs.

The Switch increments this count when it discards a frame that cannot be routed. This occurs most frequently when a destination becomes unavailable without the source realizing the destination is unavailable. There are no thresholds for this value. Typically, this occurs when the destination is not available due to the destination device's action.

- **Four Byte Words Received** — The number of four-byte words received.
- **Four Byte Words Transmitted** — The number of four-byte words transmitted.

Error Statistics

Port errors indicate that a port is not operating correctly. Use this data to isolate problems with port and link operations. The statistics in this table include:

- **Link failures** — A link failure was recorded in response to a not operational sequence (NOS), protocol timeout, or port failure. At the **Hardware** view, a yellow triangle displays to indicate a link incident, or a blinking red and yellow diamond displays to indicate a port failure.
- **Sync losses** — A loss of synchronization was detected because the attached device was reset or disconnected from the port. At the **Hardware** view, a yellow triangle displays to indicate a link incident.
- **Signal losses** — A loss of signal was detected because the attached device was reset or disconnected from the port. At the **Hardware** view, a yellow triangle displays to indicate a link incident.
- **Primitive sequence errors** — An incorrect primitive sequence was received from the attached device, indicating a Fibre Channel link-level protocol violation. At the **Hardware** view, a yellow triangle displays to indicate a link incident.
- **Discarded frames** — A received frame could not be routed and was discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the Switch.

- **Invalid transmission words** — The number of times that the Switch detected invalid transmission words from the attached device. This indicates that a frame or primitive sequence arrived at the Switch's port corrupted. This corruption can be due to the attached device performing a reset, plugging or unplugging the link, bad optics at either end of the cable, bad cable, or a dirty or poor connection. Moving the connection around or replacing cables can isolate the problem.

Some number of invalid transmission words are expected and acceptable. Invalid transmission words within a frame are used to produce the bit-error threshold link incident. If one or more invalid transmission words are detected in 12 separate 1.5-second samples within five minutes, a bit-error threshold link incident is generated.

- **CRC errors** — A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the Switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors** — The number of times that the Switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the Switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors** — A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.
- **Frames too short** — A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the Switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

Troubleshooting Tips

As a general rule, you should clear all counts after the system is stabilized. When looking at the **Performance** view, roughly keep track of the time interval when errors accumulate to judge the presence and severity of a problem. Also, recognize that there is a link recovery hierarchy implemented in Fibre Channel to handle some level of "expected anomalies." In general, only be concerned with error counts that increment very quickly.

Button Functions

The two buttons located at the right end of the title bar on the **Statistics** Values table are:

- **Clear** — The **Clear** button clears all counters to zero. Choosing this button displays a **Clear Request Confirmation** dialog box. Confirming the request clears the statistics in the hardware at the physical port. Note that this also clears counters for other Product Manager users.

An entry identifying when the statistics were cleared and by whom is saved in the **Audit Log**.

- **Refresh** — The **Refresh** button updates the data in the statistics tables and enables you to compare values at any given time. Note that you can also refresh data by clicking the port's bar graph.

Port Operational States

[Table 2–1](#) describes the port operational states and the LED and attention indicators that display in the **Hardware** view and **Port List** view.

Table 2–1: Port States and Indicators

Port State	Port Indicators		Alert Indicator ^a	Description
	Green	Amber		
Beaconing	Off or On	Blink	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to find a specific port. Enable beaconing through the port's menu on the Hardware view, Port List view, or Performance view.
Inactive	Off	Off	Yellow Triangle	The Switch port is in an inactive state. Reasons for this state display in the Reason field of the Port Properties dialog box. Note that if port optics have also failed, the amber LED will be on.
Invalid Attachment	On	Off	Yellow Triangle	The Switch port is in an invalid attachment state. Reasons for this state display in the Reason field of the Port Properties dialog box.

Table 2–1: Port States and Indicators (Continued)

Port State	Port Indicators		Alert Indicator ^a	Description
	Green	Amber		
Link Incident	Off	Off	Yellow Triangle	A link incident occurred on one of the ports and displays in the Port List view with a corresponding indicator displaying for the card in the Hardware view.
Link Reset	Off	Off	Yellow Triangle	The Switch and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is being received on the Switch port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off.
Not Operational	Off	Off	Yellow Triangle	The Switch port is receiving the Fibre Channel not operational sequence (NOS), indicating that the attached device is not operational.
Online	On	Off	None	The attached device has successfully connected to the Switch and is ready to communicate or is in the process of communicating with other attached devices. As long as the port remains in the online state, the green port LED remains illuminated. Note that on the actual port in the unit, the green LED blinks when there is active Fibre Channel traffic through the port.

Table 2–1: Port States and Indicators (Continued)

Port State	Port Indicators		Alert Indicator ^a	Description
	Green	Amber		
Offline	Off	Off	None	The Switch port was configured as “blocked” and is transmitting the Fibre Channel OLS to the attached device.
	Off	Off	Yellow Triangle	The Switch port was configured as “Unblocked” and is receiving the Fibre Channel OLS, indicating that the attached device is offline.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The Switch port has failed and requires service. The amber LED for the port remains illuminated.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented preventing the two fabrics from joining (this only occurs when two Switches are connected to each other). Display the Port Properties dialog box to view the segmentation reason.
Testing	Off	Blink	Yellow Triangle	Port is executing an internal loopback test.
	On	Blink	Yellow Triangle	Port is executing an external loopback test. Note: For any loopback test, the amber LED blinks (beacons) to help users locate the port under test.
Not Installed	Off	Off	Yellow Triangle	The port optics are not installed or the feature that provides additional port function is not enabled.

- a. The alert indicator displays on the port in the **Hardware** view. It indicates that a corrective action is required to return the port to a normal operating state.

Link Incident Alerts

A link incident is a problem detected on a fiber optic link, like the loss of light, invalid sequences, and other problems. When a problem occurs, a LIN alert is sent to the **Link Incident Log** in the Switch Product Manager. LIN alerts warn you that there is a link incident being detected through a port connection that may require operator intervention to correct.

If LIN alerts are enabled for a port in the **Configure Ports** dialog box, a yellow triangle (attention indicator) displays by the port connector in the **Hardware** view or in the **Alert** column in the **Port List** view. A corresponding triangle displays for the card on the **Hardware** view. Double-clicking the port with the yellow triangle displays the **Port Properties** dialog box.

If LIN alerts have been enabled for a port in the **Configure Ports** dialog box, the **Port Properties** dialog box contains a short description of the latest incident in the **Link Incident** field. Or, if there are no active incidents, “None” displays. The system writes all link incidents to the **Link Incident Log**.

If you enable LIN alerts for a port in the **Configure Ports** dialog box, configure e-mail notification through the HAFM, and enable **E-Mail Notification** through the **Maintenance** menu, you will receive e-mail notification of LIN alerts.

NOTE: The e-mail notification of LIN alerts is available to all users; no user rights are imposed.

Although you can clear the attention indicator in the **Hardware** view and the alert description in the **Port Properties** dialog box manually, they may also be cleared by actions outside of your control; such as on HAFM server reboot.

You can clear the link incident indicator in the **Hardware** view and the description in the **Link Incident** field manually. To manually clear the attention indicator (yellow triangle), right-click the port with the yellow triangle and choose **Clear Link Incident Alert(s)** from the menu. In the **Clear Link Incident Alert(s)** dialog box, choose the appropriate option and click **OK**.

Be aware that clearing the incident indicator clears it for everyone using the system. If there are no link incident alerts enabled for a port, no actions occur.

Threshold Alerts

A threshold alert notifies Product Manager users when the transmit (Tx) or receive (Rx) throughput reaches specific values for Switch ports or port types (E_Ports or F_Ports).

Choose the **Threshold Alerts** option on the **Configure** menu to display the **Configure Threshold Alerts** dialog box. Use this dialog box to configure criteria for generating a threshold alert. One criteria that you must configure is a throughput value that equals a specific percentage of the port's total throughput capacity. You also provide a time interval during which throughput is measured and a time interval during which that throughput value must remain constant. When throughput reaches the threshold value and remains constant for the specified time, an alert is generated.

Threshold alerts occur as the following in the Product Manager:

- An attention indicator (yellow triangle) that displays on the port in the **Port Card** view.
- An attention indicator (yellow triangle) that displays on the port card in the **Hardware** view.
- An attention indicator (yellow triangle) that displays in the **Alert** column of the **Port List** view.
- An attention indicator (yellow triangle) that displays by the **Threshold Alerts** field in the **Port Properties** dialog box.
- Detailed threshold alert data recorded in the **Threshold Alert Log**.

For detailed procedures to configure threshold alerts, refer to [Configure Threshold Alerts on page 3–28](#).

Configuring the Switch

This chapter describes how to use the options that display on the Product Manager's **Configure** menu on the **Product Manager** menu bar.

Configure Identification

Use the procedure in this section to identify the Switch by its name, description, location, and contact person. This information displays in the following Product Manager locations:

- **Product Manager** window title panel (name).
- **Switch Properties** dialog box (name, location, contact, description).
- Identification table at the top of the **Hardware** view (name, location, description).

The name also displays in the Switch icon label in the HAFM **Product** tab if the product name is enabled through the HAFM Display Options.

Data entered through the following procedure is saved in nonvolatile random access memory (NVRAM) on the Switch.

Procedure

To configure identification for the Switch, use the following steps:

1. Choose **Identification** from the **Configuration** menu on the menu bar.

The **Configure Identification** dialog box displays.



Figure 3–1: Configure Identification dialog box

2. Click in the name field and enter a name for the Switch. The name could reflect the Switch's Ethernet network domain name service (DNS) host name, if assigned.
3. Click in the description field and enter a description of the Switch.
4. Click in the location field and enter the location of the Switch.
5. Click in the contact field and enter appropriate information about a contact person, such as a phone number, title, or e-mail address.
6. Click **Set Name as Nickname** and add a check mark to the check box if you want to use the name in the **Name** field as a nickname for the Switch's WWN. The nickname will then display instead of the WWN in **Product Manager** views.
7. Click **Activate** to save the data and close the dialog box.
8. If you are finished configuring the Switch, back up the configuration data. For more information, refer to [Backup and Restore Configuration on page 5–7](#).

Configure Switch Operating Parameters

Use the procedures in this section to set parameters on the Switch for fabric operation through the **Configure Switch Parameters** dialog box. These operating parameters are stored in NVRAM on the Switch.

1. The Switch must be offline to change Preferred Domain ID and Operating Mode parameters. If it is not and you activate values in this dialog box, a dialog box displays prompting you to set the unit offline.



CAUTION: Setting the Switch offline terminates all Fibre Channel connections.

To set the unit offline:

- a. Choose **Set Online State** from the **Maintenance** menu on the menu bar along the top of the Product Manager window.
 - b. When the **Set Online State** dialog box displays, click **Set Offline**.
 - c. When the warning box displays asking you to confirm the offline state, click **OK**.
2. Choose **Switch Parameters** from the **Operating Parameters** submenu (**Configure** menu tab).
 3. The **Configure Switch Parameters** dialog box displays.

Figure 3–2: Configure Switch Parameters dialog box

NOTE: Ordinarily, you do not need to change values in this dialog box from their defaults. The only exception is the **Preferred Domain ID**. Change this value if the Switch will participate in a multiSwitch fabric.

4. Use information under the next section, [Switch Parameters](#), to change settings as required for parameters in this dialog box.
5. After you change settings, click the **Activate** button.

Switch Parameters

Configure the following parameters as required by your fabric.

Domain ID

The domain identification is a value between 1 and 31 that provides a unique identification for the Switch in a fabric. A fabric Switch cannot contain the same domain ID as another Switch or their E_Ports will segment when they try to join.

In the **Configure Switch Parameters** dialog box, a field is provided to enter a preferred domain ID and a check box is provided to enable this ID as an insistent domain ID.

Preferred

To change this value, you must first set the Switch offline. Choose **Set Online State** from the **Maintenance** menu to display the **Set Online State** dialog box, then click the **Set Offline** button. Be sure to set the Switch back online after you change this value.

Use this field to set the a unique domain ID for the Switch. The default value is 1. Set a value between 1 and 31. When a Switch comes online with a preferred ID, it requests an ID from the fabric's principal Switch (indicating its preferred value as part of the request). If the requested domain ID is not allocated to the fabric, the domain ID is assigned to the requesting Switch. If the requested domain ID is already allocated, an unused domain ID is assigned. Note that you must set the Switch offline before you can change to the preferred domain ID.

The preferred domain ID must be unique for each Director and Switch in a fabric. If two Switches or Directors have the same preferred domain ID, the E_Ports segment, causing the fabric to segment.

For more information on domain ID, refer to the section on domain ID assignment for multiSwitch fabrics in the *hp StorageWorks SAN high availability planning guide* for details.

Insistent

This option is not supported unless the SANtegrity feature is installed. Click the check box to remove or add a checkmark. The default state is disabled (no checkmark).

When a checkmark displays, the domain ID configured in the **Preferred Domain ID** field will become the active domain identification when the fabric initializes. See the following notes:

- This option is required if Enterprise Fabric mode (optional SANtegrity feature) is enabled. Refer to [Insistent Domain Identification \(ID\) on page 6-15](#) for details.
- If you enable Insistent Domain while the Switch or Director is online, the Preferred Domain ID will change to the current active domain ID if the IDs are different.



CAUTION: If a Switch with a duplicate domain ID exists in the fabric, both Switches' E_Ports will segment when they try to join.

Rerouting Delay

Placing a check mark in the check box to the left of the Rerouting Delay option enables rerouting delay. This option is only applicable if the configured Switch is in a multiSwitch fabric. The default state is disabled.

Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new Switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the **Configure Fabric Parameters** dialog box. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path.

NOTE: This option is required if Enterprise Fabric mode (optional SANtegrity feature) is enabled. Refer to [Rerouting Delay on page 6-13](#) for details.

Domain RSCNs

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. Note that this option is required if Enterprise Fabric mode (optional SANtegrity feature) is enabled. Refer to [Domain RSCNs on page 6-14](#) for details.

Operating Mode

NOTE: To change this value, you must first set the Switch offline. Choose **Set Online State** from the **Maintenance** menu to display the **Set Online State** dialog box, then click the **Set Offline** button. Be sure to set the Switch back online after you change this value.

Click either the **S/390** or **Open Systems** radio buttons:

- If the FICON Management Server feature is enabled, the default mode will be S/390. The operating mode cannot be changed to Open Systems with the FICON Management Server feature enabled. Typically, S/390 mode is used when attaching an IBM S/390 Parallel Enterprise or zSeries server to the Switch and implementing inband Switch management through a Fibre Connection (FICON) channel.
- Use Open Systems mode for all other (non-FICON) Fibre channel environments.

Configure Fabric Operating Parameters

Use procedures in this section to set parameters on the Switch for fabric operation through the **Configure Fabric Parameters** dialog box. These operating parameters are stored in NVRAM on the Switch.

1. The Switch must be offline to change parameters in this dialog box. If it is not and you activate values, a dialog box displays prompting you to set the unit offline.

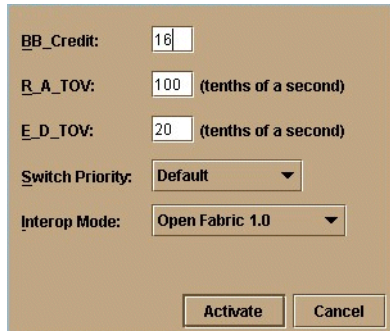


CAUTION: Setting the Switch offline terminates all Fibre Channel connections.

To set the unit offline:

- a. Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.

- b. Click **Set Offline**. A warning box displays asking you to confirm the offline state.
 - c. Click **OK**.
2. Choose **Configure > Operating Parameters > Fabric Parameters** from the **Product Manager** window. The **Configure Fabric Parameters** dialog box displays, as shown in Figure 3–3.

The image shows a 'Configure Fabric Parameters' dialog box with a tan background. It contains five configuration items: 'BB_Credit' with a text box containing '16'; 'R_A_TOV' with a text box containing '100' and '(tenths of a second)' to its right; 'E_D_TOV' with a text box containing '20' and '(tenths of a second)' to its right; 'Switch Priority' with a dropdown menu showing 'Default'; and 'Interop Mode' with a dropdown menu showing 'Open Fabric 1.0'. At the bottom right are 'Activate' and 'Cancel' buttons.

BB_Credit:	16
R_A_TOV:	100 (tenths of a second)
E_D_TOV:	20 (tenths of a second)
Switch Priority:	Default
Interop Mode:	Open Fabric 1.0
<div>Activate Cancel</div>	

Figure 3–3: Configure Fabric Parameters dialog box

NOTE: Ordinarily, you do not need to change values in this dialog box from their defaults. The only exception is the **Preferred Domain ID**. Change this value if the Switch will participate in a multiSwitch fabric.

3. Use information under “Fabric Parameters” to change settings as required for parameters in this dialog box.
4. After you change settings, click the **Activate** button.
5. Back up the configuration data when you are finished configuring the Switch.

Fabric Parameters

Configure the following parameters as required by your fabric.

BB_Credit

Configure the Switch to support buffer to buffer credit (BB_Credit) from 1 through 60. This is the value used for all ports, except those configured for extended distance buffering (10-100 km). The default value is 16. For a description of the buffer-to-buffer credit, refer to the industry specification, *Fibre Channel Physical and Signaling Interface*.

R_A_TOV

Configure resource allocation time-out value (R_A_TOV) in tenth-of-a-second increments. This variable works with the error detect time-out value (E_D_TOV) variable to control the Switch's behavior when an error condition occurs. Resources are allocated to a circuit when errors are detected and are not released for reuse until the time set by the R_A_TOV value expires. The default value is 100 tenths (10 seconds). Set a value between 10 tenths and 1200 tenths (1 through 120 seconds).

NOTE: Set the same value for R_A_TOV on all Directors and Switches in a multiSwitch fabric. If the value is not the same on all units, the fabric segments. Also, the value for R_A_TOV must be greater than the value configured for E_D_TOV.

E_D_TOV

Adjust the E_D_TOV in tenth-of-a-second increments. An error condition occurs when an expected response is not received within the time limit set by this value. The default value is 20 tenths (2 seconds). Set a value between 2 tenths through 600 tenths (.2 through 60 seconds).

NOTE: Set the same value for E_D_TOV on all Switches and Directors in a multiSwitch fabric. If the value is not the same, the fabric segments.

Switch Priority

Setting this value determines the principal Switch for the multiswitch fabric. Choose **Principal** (highest priority), **Default**, or **Never Principal** (lowest priority) from the **Switch Priority** drop-down list.

Setting these priority values determines the principal Switch selected for the multiswitch fabric. For example, if you have three Switches in the fabric and set one as **Principal**, one as **Default**, and one as **Never Principal**, the unit set to **Principal** becomes the principal Switch in the fabric.

If all Switches are set to **Principal** or **Default**, the Switch with the highest priority and the lowest WWN becomes the principal Switch. Following are some examples of principal Switch selection when Switches have these settings:

- If you have three Switches and set all to **Default**, the Switch with the lowest WWN becomes the principal Switch.
- If you have three Switches and set two to **Principal** and one to **Default**, the Switch with the **Principal** setting that has the lowest WWN becomes the principal Switch.
- If you have three Switches and set two to **Default** and one to **Never Principal**, the Switch with the **Default** setting and the lowest WWN becomes the principal Switch.

At least one Switch in a multiswitch fabric needs to be set as **Principal** or **Default**. If all of the Switches are set to **Never Principal**, all of the interswitch links (ISLs) will segment. If all but one Switch is set to **Never Principal** and the Switch that was principal goes offline, then all of the other ISLs will segment.

NOTE: We recommend you leave the Switch priority setting as **Default**. If you are considering setting this value to something other than the default, refer to the section on principal Switch selection for multiSwitch fabrics in the *hp StorageWorks SAN high availability planning guide* for details.

In, for example, the audit log, you may notice that the **Principal** setting maps to a number code of 1, **Default** maps to a number code of 254, and **Never Principal** maps to a number code of 255. The number codes of 2 - 253 are not currently in use.

Interop Mode

Choose the following option:

- **Open Fabric 1.0.** Choose this mode if the fabric contains HP Directors and Switches, as well as other open-fabric compliant Switches. Choose this mode for managing heterogeneous fabrics.

Configure Ports

Use the procedures in this section to configure names, blocked and unblocked state, 10-100 km extended distance buffering, enable or disable link incident (LIN) alerts for ports, port type, port speed, Port binding, and WWN binding name.

Port configuration data is stored in NVRAM on the Switch. Configure data in the following columns of the **Configure Ports** dialog box:

- **Port #** — You cannot edit this field. This column identifies the port number. The port numbers range from 0 through 31.
- **Name** (Open Systems mode only) — Enter a name for the port. The port names display in the **Port Properties** dialog box and elsewhere in the Product Manager to identify the port.

NOTE: To identify port numbers for which you want to provide names, place the cursor over the ports in the **Hardware** view. As you move over a port, a message displays that identifies the slot number where the port is installed.

To name ports in S/390 mode, use the **Configure Addresses** dialog box.

- **Blocked** (open systems mode only) — Placing a check mark in the check boxes of this column blocks the operation of the port.

To block ports in S/390 mode, use the **Configure Addresses** dialog box.

- **10-100Km** — This column is for extended distance buffering. You can enable extended distance for a port even if it is not an extended distance port. However, enabling extended distance buffering on a port disables the ability for the port to send broadcast traffic. When you choose this option, the port can support up to 60 buffer-to-buffer credits (BB_Credits) to handle link distances up to 100 km. This enables the port to process 2K frames from attached devices. If this option is not enabled, the port uses the BB_Credit (1-60) configured through the **Operating Parameters** dialog box.

If a device is connected and logged in to the fabric when extended distance is enabled or disabled on the corresponding port, the Switch will send OLS for 5 milliseconds to force the device to log in again and obtain the new BB_Credit value set for the port.

- **LIN Alerts** — A link incident (LIN) is a problem detected on a fiber optic link, such as the loss of light or invalid sequences. When a problem occurs, a LIN alert is sent to the **Link Incident Log** in the Switch Product Manager. LIN alerts warn you that there is a link incident being detected through a port connection.

Place or remove check marks in the check boxes in this column to enable or disable link incident alerts. The factory default is to enable LIN alerts.

A link incident causes a yellow attention indicator (triangle) to display for the port in the **Hardware** view and in the alert column of the **Port List** view. Once a LIN occurs, you must acknowledge it by choosing the **Clear Link Incident Alert** option from the right-click menu for the port (**Hardware** view). A description of the alert displays in the **Link Incident** field of the **Port Properties** dialog box (refer to [Figure 2-3](#)).

If the check boxes in this column are not selected, no link incident indicators display in the **Hardware** view. Also, the **Link Incident** field of the **Port Properties** dialog box is blank and a link incident is recorded in the Link Incident Log. LINs are always logged in the regardless of the configuration.

If LIN Alerts are enabled, you can receive e-mail notification when a LIN occurs. In order to receive e-mail notification, you must configure and enable this feature in the HAFM (**Maintenance** menu) and enable e-mail notification through the **Enable E-Mail Notification** option on the Product Manager's **Maintenance** menu.

For additional information about LIN alerts, refer to [Link Incident Alerts on page 2-39](#).

- **Type** (Open Systems mode only) — Choose each port's type (**G_Port**, **E_Port**, or **F_Port**) in this column from the drop-down list.

NOTE: In S/390 mode, you cannot change port types unless the optional SANtegrity feature is installed. If ports are configured as E_Ports in Open Systems mode, and you install SANtegrity before changing to S/390 mode, the ports will remain as E_Ports when you change to S/390 mode. If SANtegrity is not installed, setting a Switch to S/390 mode will change all E_ports to G_Ports.

- **Port Binding** — Click this check box to display a check mark and enable Port binding for the port. This allows only a specific device to attach to the port. This device is specified by the WWN or nickname entered into the column. With the check box cleared, any device can attach to the port even if a WWN or nickname is specified in the column.
- **Speed** — Click the **Speed** column for a specific port, and choose **2 Gb/sec**, **1 Gb/sec**, or **Negotiate**. This sets the data rate for the port. Choosing "Negotiate" allows the port to negotiate the data speed with an attached device. Follow the rule specified in the following note when setting the data speed:

NOTE: Only set the speed to **2 Gb/sec** on ports that support this speed. If the port optics do not support **2 Gb/sec**, a warning displays stating that the optical transceiver in the port does not support the data rate.

When you change a port's speed and click **Activate** on the dialog box, a confirmation message displays stating that this setting will temporarily disrupt port data transfers.

- **Bound WWN** — Enter a World Wide Name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through the *HAFM* application. The device with this WWN or nickname will have exclusive attachment to the port if **Port Binding** is enabled. If a valid WWN or nickname is not entered in this field, but the **Port Binding** check box is checked (enabled), then no devices can connect to the port. If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can connect to the port.

Procedure (Open Systems mode)

To configure ports in Open Systems mode, use the following steps:

1. Choose **Ports** from the **Configure** menu on the menu bar.

The **Configure Ports** dialog box displays.

Port #	Name	Blocked	10-100 km	LIN Alerts	Type	Speed	WWN Binding	Bound WWN
0		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:00:00:00:C9:00:00:00
1		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:01:00:60:48:00:00:00
2		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:02:00:00:C9:00:00:00
3		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:03:00:60:48:00:00:00
4		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:04:00:E0:69:00:00:00
5		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:05:00:00:C9:00:00:00
6		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:06:00:00:C9:00:00:00
7		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:07:00:60:48:00:00:00
8		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:08:00:00:20:00:00:00
9		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:09:00:60:48:00:00:00
10		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:0A:00:60:48:00:00:00
11		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:0B:00:00:C9:00:00:00
12		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:0C:08:00:20:00:00:00
13		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:0D:00:00:C9:00:00:00
14		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:0E:00:00:C9:00:00:00
15		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:0F:08:00:20:00:00:00
16		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:10:08:00:20:00:00:00
17		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:11:00:60:48:00:00:00
18		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:12:00:00:C9:00:00:00
19		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:13:08:00:20:00:00:00
20		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:14:00:E0:69:00:00:00
21		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input checked="" type="checkbox"/>	20:15:00:00:C9:00:00:00
22		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:16:00:00:C9:00:00:00
23		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	20:17:08:00:20:00:00:00

Figure 3–4: Configure Ports dialog box

Ports are numbered from 0 through 31.

2. Click a **Name** field and type a name that reflects the end device connected through the port. For example, use “XYZ Server,” where XYZ is the brand name of the server.

3. Block or unblock operation for a port by clicking the check box in the **Blocked** column. When a check mark displays, the port is blocked.
4. Enable or disable extended distance buffering for the port by clicking the check box in the **10-100 km** column. When a check mark displays, extended distance buffering is enabled.
5. Enable or disable LIN alerts for the port by clicking the check box in the **LIN Alerts** column. When a check mark displays, LIN alerts are enabled.

NOTE: The factory default for LIN alerts is enabled.

6. Choose a port type by clicking in the **Type** field and choosing from the list.
7. To bind a device with a specific WWN or nickname to the port, click the **Port Binding** check box to display a check mark. Then enter the WWN or configured nickname for the device into the **Bound WWN** column. The device that you bind to the port will have exclusive connection to that port.

Notes

- If you have configured port binding and click **Activate**, a warning dialog box displays if one or more of the nodes attached to a port does not match the WWN or nickname configured in the **Bound WWN** column. This warning box displays a list of all attached nodes that will be logged off if you continue. If you click, these nodes will log off and the port will only attach to the device with the WWN or nickname configured in the **Bound WWN** column.
 - If you have configured port binding and click **Activate**, an error message may display if the format for the WWN entered in the **Bound WWN** column is not valid (not in xx.xx.xx.xx.xx.xx.xx.xx format) or if you enter a nickname that has not been configured through the Product Manager.
8. To set the data speed for the port, click in the **Speed** column for the port, and choose, **2 Gb/sec**, **1 Gb/sec**, or **Negotiate**. Choosing **Negotiate** allows the port and attached device to negotiate the data rate.
 9. Use the scroll bar on the right side of the **Configure Ports** dialog box table to display additional ports that you want to configure.
 10. Activate changes and close the dialog box by clicking **Activate**.
 11. If you are finished configuring the Switch, back up the configuration data. For more information, refer to [Backing Up and Restoring Configuration Data on page 3-37](#).

Procedure (S/390 mode)

To configure ports in S/390 mode, use the following steps:

1. Choose **Ports** from the **Configuration** menu on the menu bar.

The **Configure Ports** dialog box displays.

Port #	10-100 km	LIN Alerts	WWN Binding	Speed	Bound WWN
0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:00:00:00:C9:00:00:00
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:01:00:60:48:00:00:00
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:02:00:00:C9:00:00:00
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:03:00:60:48:00:00:00
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:04:00:E0:69:00:00:00
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:05:00:00:C9:00:00:00
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:06:00:00:C9:00:00:00
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:07:00:60:48:00:00:00
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:08:08:00:20:00:00:00
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:09:00:60:48:00:00:00
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:0A:00:60:48:00:00:00
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:0B:00:00:C9:00:00:00
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:0C:08:00:20:00:00:00
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:0D:00:00:C9:00:00:00
14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:0E:00:00:C9:00:00:00
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:0F:08:00:20:00:00:00
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:10:08:00:20:00:00:00
17	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:11:00:60:48:00:00:00
18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:12:00:00:C9:00:00:00
19	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:13:08:00:20:00:00:00
20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:14:00:E0:69:00:00:00
21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 Gb/sec	20:15:00:00:C9:00:00:00
22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:16:00:00:C9:00:00:00
23	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1 Gb/sec	20:17:08:00:20:00:00:00

Figure 3–5: Configure Ports dialog box (S/390 Mode)

Ports are numbered from 0 through 15.

2. Enable or disable extended distance buffering for the port by clicking the check box in the **10-100 km** column. When a check mark displays, extended distance buffering is enabled.
3. Enable or disable LIN alerts for the port by clicking the check box in the **LIN Alerts** column. When a check mark displays, LIN alerts are enabled.

NOTE: The factory default for LIN alerts is enabled.

4. To bind a device with a specific WWN or nickname to the port, click the **WWN Binding** check box to display a check mark. Then enter the WWN or configured nickname for the device into the **Bound WWN** column. The device that you bind to the port will have exclusive connection to that port.

Notes:

- If you have configured port binding and click **Activate**, a warning dialog box displays if one or more of the nodes attached to a port does not match the WWN or nickname configured in the **Bound WWN** column. This warning box displays a list of all attached nodes that will be logged off if you continue. If you click **Continue**, these nodes will log off and the port will only attach to the device with the WWN or nickname configured in the **Bound WWN** column.
 - If you have configured port binding and click **Activate**, an error message may display if the format for the WWN entered in the **Bound WWN** column is not valid (not in xx.xx.xx.xx.xx.xx.xx.xx format) or if you enter a nickname that has not been configured through the Product or Fabric Manager.
5. To set the data speed for the port, click in the **Speed** column for the port, and choose **1 Gb/sec**, **2 Gb/sec**, or **Negotiate**. Choosing **Negotiate** allows the port and attached device to negotiate the data rate.
 6. Use the scroll bar on the right side of the **Configure Ports** dialog box table to display additional ports that you want to configure.
 7. Activate changes and close the dialog box by clicking **Activate**.
 8. If you are finished configuring the Switch, back up the configuration data. For more information, refer to [Backup and Restore Configuration on page 5–7](#).

Configure Port Addresses (S/390 mode only)

Use this procedure to create and activate port address configurations.

Parameters

- **Addr** — This read-only field lists the port's address.
- **Port Name** — This user-defined name is assigned to the address. Up to 24 alphanumeric characters are allowed, including spaces, hyphens and underscores.

- **Blocked** — If the box is checked, the port is blocked. Blocked ports continuously transmit offline sequences (OLS), but cannot communicate to an attached device. If the box is not checked, the port is unblocked.
- **Port connection array** — This yellow area of the dialog box is a matrix of port addresses that is used to configure connections between port addressees. Each port in the Switch has a corresponding port address which equals the physical port number plus four. Therefore, the address for port 0 is 4 (0+4).

All port addresses for the Switch are listed along the top and left side of the matrix. The intersection between a vertical and horizontal row of cells (squares) is where you can either allow or prohibit connections between two addresses by clicking the cell to prohibit connection or right-clicking the cell and displaying a menu of attributes.

The default state of a cell is an empty cell (square), which represents an allowed connection. The symbol for a prohibited connection is shown in [Figure 3–6](#). Click a cell to add the prohibited symbol and prohibit connection to that cell.



Figure 3–6: Prohibited Port Connection symbol

Move your cursor over the squares in the array to display the corresponding address. Right-click the array to display the following menu options:

- **Prohibit row** — Prohibits connection between all addresses in a row. In effect, this prohibits connection between a specific address and all other port addresses.
- **Allow row** — Allows connection for all port addresses on a row that are currently prohibited. This allows connection between a port with a specific address and other allowed ports.
- **Prohibit all** — Prohibits connection between all port addresses. In this state, ports in the Switch cannot connect with any other port address.
- **Allow all** — This allows a dynamic connection through all port addresses from which connection is currently prohibited. The allowed attribute has the lowest precedence and does not override any other attribute.
- **Block all ports** — Blocks communication between all ports. Ports that are blocked continuously transmit offline sequences (OLS).

- **Unblock all ports** — Unblocks all port addresses that are currently blocked. This allows communication from all port addresses in the Switch.
- **Clear all** — Clears the prohibit and blocked status of all port addresses in the Switch.
- **CUP Name** — This user-defined name is assigned to the control unit port (CUP). Up to 24 alphanumeric characters allowed, including spaces, hyphens and underscores. A space character is not allowed as the first character, and the characters are case-sensitive. This is not a required field.
- **Activate** — Click this button to activate the current configuration. A warning displays before the action occurs.
- **Save As** — Click this button to save the current configuration with a name and description. The saved configuration will be stored on the HAFM Server and in the **Address Configuration Library**. Refer to [Manage Stored Address Configurations on page 3-19](#) for information on accessing this library.
- **Cancel** — Click this button to cancel the configuration settings and close the dialog box without saving. If you click this button after clicking the **Save As** button, your changes will be saved, and the dialog box will simply close.

Procedure

To configure, save, and activate port addresses, use the following steps:

1. Choose **Addresses** from the **Configure** menu on the menu bar, then choose **Active**.

The **Configure Addresses - “Active”** dialog box displays.

Addr	Port Name	Blocked	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13
04		<input checked="" type="checkbox"/>									⊗							
05		<input type="checkbox"/>				⊗					⊗							
06		<input checked="" type="checkbox"/>									⊗							
07		<input type="checkbox"/>			⊗						⊗							
08		<input type="checkbox"/>									⊗							
09		<input type="checkbox"/>									⊗							
0A		<input type="checkbox"/>									⊗							
0B		<input type="checkbox"/>									⊗							
0C		<input checked="" type="checkbox"/>	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
0D		<input type="checkbox"/>									⊗							
0E		<input type="checkbox"/>									⊗							
0F		<input checked="" type="checkbox"/>									⊗							
10		<input type="checkbox"/>									⊗							
11		<input type="checkbox"/>									⊗							
12		<input type="checkbox"/>									⊗							
13		<input type="checkbox"/>									⊗							

CUP Name:

Activate Save As... Cancel

Figure 3-7: Configure Addresses dialog box

2. Enter information into the appropriate fields.
3. Click the squares to either prohibit or allow connections. In [Figure 3-7](#), port address 07 is prohibited from communicating with port address 05. Also, Port 0C is prohibited from communicating with all other port addresses.
4. Click **Save As** to open the **Save Address Configuration As** dialog box.
5. Enter a name and description.

Names must be between 1 and 8 characters in length. Valid characters are uppercase A-Z, 0-9, hyphen (-), and underscore (_). The name may not be CON, AUX, COMn (where n=1-4), LPTn (where n=1-3), NUL, or PRN.

Descriptions must be between 0 and 24 characters in length. Up to 24 alphanumeric characters allowed, including spaces, hyphens and underscores.

6. Click **OK** to save changes and to close the **Save Address Configuration As** dialog box.
7. In the **Configure Addresses - “Active”** dialog box, click **Activate** to activate the configuration or click **Cancel** to close without activating.

NOTE: If you click **Cancel** after saving, your configuration will still be added to the library without being activated.

Manage Stored Address Configurations

(S/390 mode only) Once addresses configurations are created through the **Configure Addresses - “Active”** dialog box they are saved to the **Address Configuration Library**. Use this procedure to manage up to 32 address configurations in the **Address Configuration Library**.

Procedure

To manage saved library entries:

1. Choose **Addresses**, then choose **Stored** from the **Configuration** menu on the menu bar.

The **Address Configuration Library** dialog box displays.

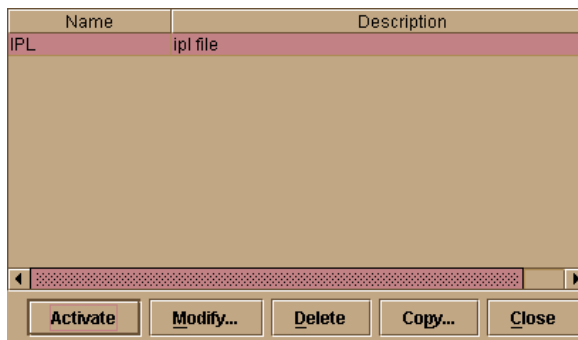


Figure 3–8: Address Configuration Library dialog box

2. Choose a configuration entry by clicking on the row. Then use one of the procedures below.
 - a. To modify a stored configuration:

Click **Modify**. The **Configure Addresses** dialog box displays for the configuration. See [Configure Port Addresses \(S/390 mode only\) on page 3-15](#) for details on using this dialog box.
 - b. To delete a stored configuration:

Click **Delete**. A warning displays before deletion.
 - c. To copy a stored configuration:

Click **Copy** to copy the configuration and rename/describe it.

When the **Copy Address Configuration** dialog box displays, provide a name and description for the configuration. Names must be between 1 and 8 characters in length. Valid characters are uppercase A-Z, 0-9, hyphen (-), and underscore (_). The name may not be CON, AUX, COMn (where n=1-9), LPTn (where n=1-9), NUL, or PRN. Descriptions must be between 0 and 24 characters in length. Up to 24 alphanumeric characters are allowed, including spaces, hyphens, and underscores. Click **OK** and the configuration is added to the library.
 - d. Activate a stored configuration
- Click **Activate** to activate the configuration and send it to the Switch for immediate use. A warning displays before the action occurs.
- NOTE:** If **Active=Saved** is enabled in through the **Configure FICON Management Server** dialog box (**Configure** menu), this overwrites the current IPL address configuration.
3. When finished managing the library, click **Close** to close the dialog box.

Configure SNMP

Use the procedures in this section to:

- Configure the SNMP agent that runs on the Switch and implements the following MIBs:
 - MIB-II.
 - Fabric Element MIB.
 - Fibre Alliance (FCMGMT) MIB.
 - Switch private MIB.

For complete information on objects defined in MIBs and steps to download MIB variables to your SNMP workstation, refer to the *hp StorageWorks SNMP reference guide for directors and edge switches*.

- Configure network addresses and community names for up to six SNMP trap recipients.

An SNMP trap recipient is a network management station that receives messages through SNMP for specific events that occur on the Switch.

- Define SNMP community names that SNMP managers use for reading variables.
- Authorize write permissions for writable MIB variables.

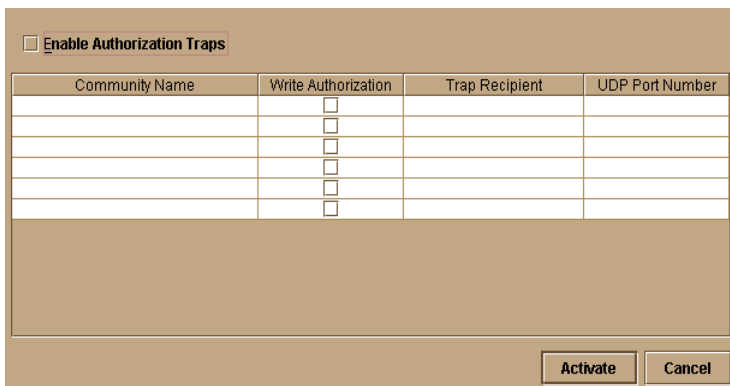
NOTE: SNMP managers may request, but will not receive, traps and SNMP data through SNMP management stations that are not configured with community names.

Procedure

To configure SNMP traps and assign community names, use the following steps:

1. Choose **SNMP** from the **Configure** menu on the menu bar.

The **Configure SNMP** dialog box displays.



Community Name	Write Authorization	Trap Recipient	UDP Port Number
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Figure 3-9: Configure SNMP dialog box

2. Click the **Enable Authorization Traps** field to enable authorization traps to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the Switch.
3. Click a field in the **Community Name** column to choose the row. Enter the SNMP community name for the trap recipient. Enter up to 32 characters. This also defines community names from which SNMP managers can read MIB variables from or write MIB variables to the Switch. Refer to the note under [Configure SNMP on page 3-21](#) for more information about assigning community names.
4. Click the **Write Authorization** check box to enable write authorization for the community name. A check mark displays in the box to indicate that write authorization is enabled.
5. Enter the IP address for a trap recipient (SNMP management station) by clicking in the **Trap Recipient** column and entering an IP address.

NOTE: Step 6 usually is not necessary. If you do not wish to override the default UDP number, skip to step 7.

6. Enter user datagram protocol (UDP) port numbers in the **UDP Port Number** column. You can override the default UDP port number of 162 with any legal UDP port number (1 to 65535).
7. Click **Activate** to activate the data and close the dialog box.
The SNMP configuration is stored in NVRAM on the Switch.
8. If you are finished configuring the Switch, back up the configuration data. For more information, refer to [Backup and Restore Configuration on page 5–7](#).

Configure Optional Features

The HAFM offers four optional features that you can configure through HAFM applications. There are two types of features:

- “Keyed” features, requiring feature keys to be purchased and enabled through the **Configure Feature Key** dialog box in the product’s *Product Manager* application.
- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through *HAFM* or *Product Manager* applications.

The optional features are as follows:

- FICON Management Server—keyed feature
- Open System Management Server (OSMS)—keyed feature
- SANtegrity—keyed feature
 - Fabric Binding
 - Switch Binding
- Enterprise Fabric Mode—non-keyed feature

These features are discussed in detail in [Chapter 6, Optional Features](#).

The next section, [Configure Feature Key](#), tells you how to setup, configure, and activate the feature key.

Configure Feature Key

A feature key is a string of alphanumeric characters consisting of both uppercase and lowercase. The following is an example of a feature key format:

XxXx-XXxX-xxXX-xX.

NOTE: The total number of characters may vary. The key is case sensitive and must be entered exactly, including the dashes.

The feature key, which is encoded with a Switch's serial number, can only be configured on the Switch to which it is assigned.

To enable an optional feature on the Switch, first set the Switch offline, then enter the feature key into the **New Feature Key** dialog box.

Display this dialog box by choosing **Feature** from the **Configure** menu on the menu bar.

FICON Management Server Feature: If you are enabling the FICON Management Server feature, the operating mode automatically configures to S/390 mode. You cannot change the operating mode to open systems mode with the FICON Management Server feature is enabled.

Procedure

To configure a feature key, use the following steps:

1. Set the Switch offline using the **Set Online State** dialog box.
 - a. Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.
 - b. Click **Set Offline**. A warning box displays asking you to confirm the offline state.
 - c. Click **OK**.
2. Choose **Configure > Features** from the **Product Manager** window. The **Configure Feature Key** dialog box displays, as shown in [Figure 3-10](#).

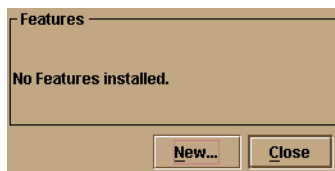


Figure 3-10: Configure Feature Key dialog box

3. Click **New** to add a new feature key. The **New Feature Key** dialog box displays, as shown in Figure 3–11.



Figure 3–11: New Feature Key dialog box

4. Enter the Switch's feature key in the **Key** field and click **OK**.
 - Feature keys are only valid for a Switch with a specific serial number. They cannot be interchanged between Switches. If an error stating "Invalid serial number" displays, verify that you have entered the feature key that was assigned to the Switch. To verify, check the serial number of the Switch through the **Switch Properties** dialog box and compare it to the serial number listed in the documentation provided with your feature key.
 - The feature key is a string of alphanumeric characters with dashes. The key is case-sensitive, so enter the key exactly as printed in the documentation that you received for the feature. If an error stating "Invalid feature key" displays, verify that you have entered the feature key correctly.

The **Enable Feature Key** dialog box displays with a warning, stating that this action will override the current set of features on the Switch. The list in the left column of the dialog box is a list of features that are active on the Switch. The list on the right is a set of features that come with the new feature key. All of the features that are active are included in the new feature list.

5. Click **Activate** to activate the new feature key.

An IPL will occur, during which the Ethernet connection between the HAFM Server and Switch is momentarily interrupted.

NOTE: If you click **Activate**, all current features will be replaced with new features. That is, if there are features shown in the current list that are not shown in the new list, then those features will be removed from the Switch.

6. Set the Switch back online.
 - a. Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.
 - b. Click **Set Online**. A warning box displays asking you to confirm the online state.
 - c. Click **OK**.
7. When you are finished configuring the Switch, you can back up the configuration data.

Configure Date and Time

Use the procedures in this section to display and change the date and time set on the Switch. You must set the current date and time on the Switch using this dialog box so the correct time stamps display in the **Event Log**, **Audit Log**, **Hardware Log**, **Link Incident Log**, and **Threshold Alerts Log**.

S/390 mode only. If both periodic synchronization and Switch clock alert mode are enabled, an error will result. Disable one of them to fix the error. Refer to the following procedure to disable periodic synchronization. Refer to [Configure Feature Key on page 3-24](#) to disable Switch clock alert mode.

Procedure

Set the Switch date and time using the following steps:

1. Choose **Date/Time** from the **Configure** menu on the menu bar.

The **Configure Date and Time** dialog box displays.

If the **Periodic Date/Time Synchronization** check box in the **Configure Date and Time** dialog box is selected, the HAFM server periodically synchronizes the Switch time to the HAFM server, and daylight savings time automatically updates. When the **Periodic Date/Time Synchronization** option is selected, the **Date** and **Time** fields are disabled (grayed out).

If the **Periodic Date/Time Synchronization** check box is not selected, you can set the HAFM server date and time manually.

Figure 3-12: Configure Date and Time Periodic Synchronization dialog box

To disable **Periodic Date/Time Synchronization**, click the check box to remove the check mark, then click **Activate**. To re-enable **Periodic Date/Time Synchronization**, click the check box to display the check box, then click **Activate**.

NOTE: Click **Activate** to synchronize the date and time at the next update period. Click **Sync Now** to synchronize the date and time immediately.

2. Perform one of the following options:

Option 1: To immediately synchronize the Switch date and time with the HAFM server, click **Sync Now**. Make sure that a check mark is in the **Periodic Date/Time Synchronization** check box.

NOTE: If you click **Activate**, the date and time synchronize at the next update period.

Option 2: To synchronize the Switch date and time with a specific date and time that you enter:

- a. Make sure that **Periodic Date/Time Synchronization** is disabled (no check). Refer to [Figure 3-13](#).

Figure 3-13: Configure date and time manually

- b. Click in a **Date** or **Time** field that you want to change.
- c. Delete characters and enter new ones as required or highlight the existing character by dragging the mouse cursor over the character and typing the new character.

NOTE: When entering the hours, use the range of 0 to 23, for minutes and seconds, use the range of 0 to 59.

- d. Click **Activate** to set the date and time on the Switch.
3. If you are finished configuring the Switch, back up the configuration data. For more information, refer to [Backing Up and Restoring Configuration Data on page 3-37](#).

Configure Threshold Alerts

A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific Switch ports or port types, (E_Ports or F_Ports).

You are notified of a threshold alert by:

- An attention indicator (yellow triangle) that displays on the port in the **Hardware** view.
- An attention indicator (yellow triangle) that displays in the **Alert** column of the **Port List** view.

An attention indicator (yellow triangle) that displays by the **Threshold Alerts** field in the **Port Properties** dialog box.

- Detailed threshold alert data recorded in the **Threshold Alert Log**.

Use the **Threshold Alerts** option on the **Configure** menu to configure the following:

- Name for the alert.
- Type of threshold for the alert (Rx, Tx, or either).
- Active or inactive state of the alert.

- Threshold criteria:
 - Percent traffic capacity utilized. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value. For example the value of 50 means that the port's threshold is reached when throughput reaches 50% of port capacity.
 - Time interval during which throughput is measured and alert notification can occur.
 - The maximum cumulative time that throughput percentage can be exceeded during the set time interval before an alert is generated.
- Ports for which you are configuring threshold alerts.

You can configure up to 16 alerts, and any number of alerts can be active at one time.

Procedure

Use the following procedures to create a new threshold alert, or to modify, activate, deactivate, or delete an alert.

Create New Alert

1. Choose **Threshold Alerts** from the **Configure** menu on the menu bar.

The **Configure Threshold Alerts** dialog box displays.

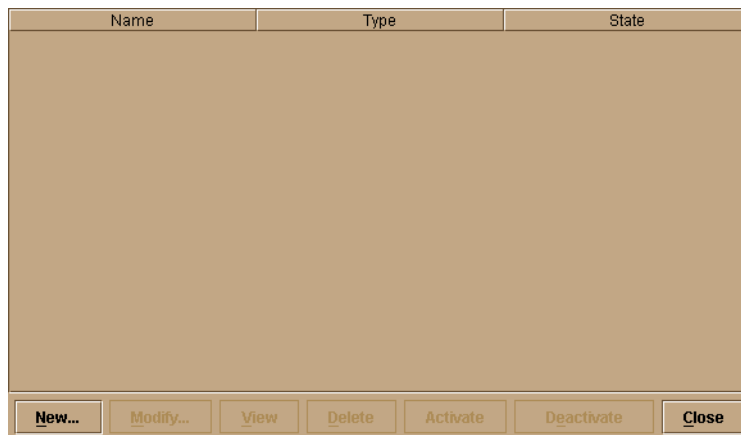


Figure 3–14: Configure Threshold Alerts dialog box

If alerts are configured, they will display in table format showing the name of the alert, type of alert (Rx, Tx, or Rx or Tx), and alert state (inactive or active).

2. Click **New**.

The **New Threshold Alert** dialog box displays.

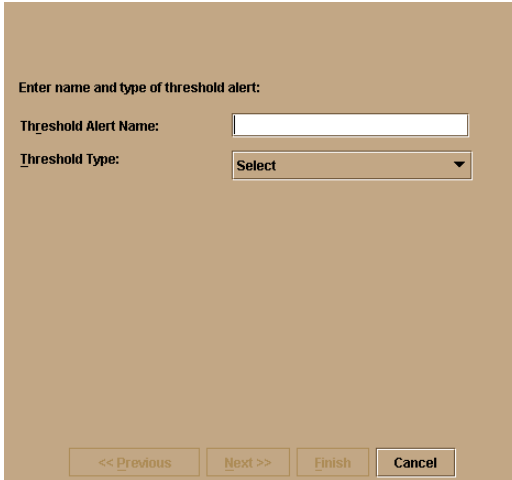
The image shows a dialog box titled "New Threshold Alerts dialog box - first screen". It has a tan background. At the top, it says "Enter name and type of threshold alert:". Below this, there are two fields: "Threshold Alert Name:" followed by a text input box, and "Threshold Type:" followed by a dropdown menu with "Select" and a downward arrow. At the bottom, there are four buttons: "<< Previous", "Next >>", "Finish", and "Cancel".

Figure 3–15: New Threshold Alerts dialog box - first screen

3. Enter a name from one to 64 characters in length. All characters in the ISO Latin-1 character set, excluding control characters, are allowed.
4. Choose one of the following from the drop-down list under the **Name** field:
 - **Rx Throughput.** An alert will occur if the threshold set for receive throughput is reached.
 - **Tx Throughput.** An alert will occur if the threshold set for transmit throughput is reached.
 - **Rx or Tx Throughput.** An alert will occur if the threshold set for either receive or transmit throughput is reached.
5. Click **Next**.

A new screen displays with additional parameters. The name configured for the alert displays at the top of the screen.

(Click **Previous** if you need to return to the previous screen.)

Generate a Threshold Alert named "Port 15 Alert", if Tx Throughput reaches:

15 % utilization

☐ At any time

☒ For 4 cumulative minutes or more

during the 10 minute notification interval.

<< Previous Next >> Finish Cancel

Figure 3–16: New Threshold Alerts dialog box - second screen

6. Enter a percentage from 1 through 100 for **% utilization**. When throughput reaches this percentage of port capacity, a threshold alert will occur.
7. Enter the amount of cumulative minutes in which the **% utilization** should exist during the notification interval before an alert is generated. You can also choose **At any time** if you want an alert to occur whenever the set **% utilization** is reached. The valid range is 1 to the interval set in step 8 (following).
8. Enter the interval in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.
9. Click **Next**.

A new screen displays for choosing ports for the alerts.

Select port(s) to run threshold alert on:

☐ Port Type

☐ E_Ports

☐ F_Ports

☒ Port List

☐ Port 10

☐ Port 11

☐ Port 12

☐ Port 13

☐ Port 14

☒ Port 15

Set All Ports

Clear All Ports

<< Previous Next >> Finish Cancel

Figure 3–17: New Threshold Alerts dialog box - third screen

10. Either choose **Port Type** or **Port List**.

- If you choose **Port Type**, choosing either E_Ports or F_Ports will cause this alert to generate for all ports configured as E_Ports or F_Ports respectively.
- If you choose **Port List**, you can choose individual ports by clicking the check box by each port number or set all ports. Choosing **Set All Ports** places a check mark by each port number. Choosing **Clear All Ports** will clear the check marks by each port number.

11. Click **Next**.

A final screen displays to provide a summary of your alert configuration. To make any changes, backwards and forwards through the configuration screens by choosing the **Previous and Next buttons**.

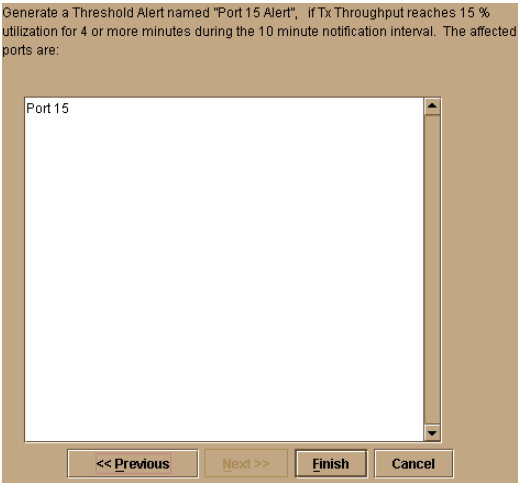


Figure 3-18: New Threshold Alerts dialog box - summary screen

12. Choose **Finish**.

The **Configure Threshold Alerts** dialog box displays listing the name, type, and state of the alert that you just configured.

13. At this point, the alert is not active. To activate the alert, choose the alert information that displays in the **Configure Threshold Alerts** table and choose **Activate**.

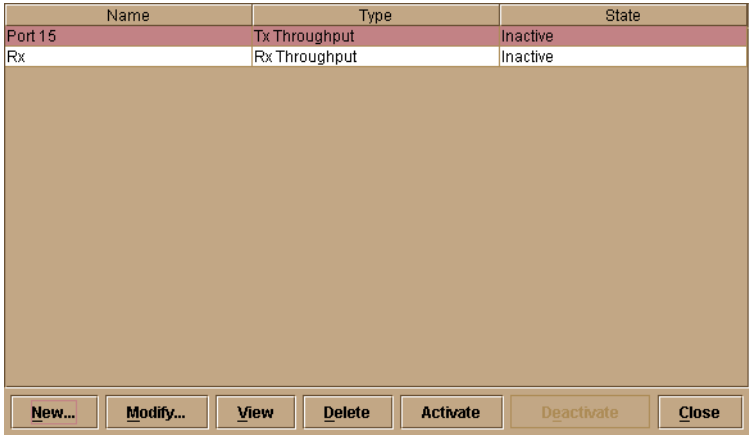


Figure 3-19: Configure Threshold Alerts dialog box - alert activated

Modify an Alert

Use the following steps to modify an existing threshold alert configuration.

1. Choose **Threshold Alerts** from the **Configure** menu.
The **Configure Threshold Alerts** dialog box displays.
2. Choose the alert that you want to modify by clicking the alert information in the table.
3. If the alert is active, choose **Deactivate**, then choose the alert information in the table again.
4. Choose **Modify**.

NOTE: If the alert is active, an error message displays prompting you deactivate the alert.

An initial **Modify Threshold** screen displays where you can change the threshold type.

5. Choose a threshold type from the drop-down list.
6. Choose **Next** when you are done. A **Modify Threshold** screen displays where you can change the % utilization, cumulative minutes for the threshold to occur before notification, and the time interval for measuring throughput and for alert notification.
7. Continue through the **Modify Threshold** screens until the summary screen displays displaying the alert configuration.
8. Perform either of the following steps:
 - If you need to change any parameters, choose **Previous** and **Next** to display the desired **Modify Threshold** screen.
 - Choose **Finish** when you are done.

Activate or Deactivate Alerts

Use the following steps to activate or deactivate existing threshold alerts. In the active state, notifications are generated for the alert. In the inactive state, notifications do not occur.

1. Choose **Threshold Alerts** from the **Configure** menu.
The **Configure Threshold Alerts** dialog box displays. The port's current state, deactivate or active, is listed under the **State** column.

2. To change the state, choose the alert by choosing the alert information in the table.
3. If the alert is active, choose **Deactivate** to change to the deactive state. If the alert is deactive, choose **Activate** to change to the active state.

Delete Alerts

Use the following steps to delete existing threshold alerts.

1. Choose **Threshold Alerts** from the **Configure** menu.

The **Configure Threshold Alerts** dialog box displays.

2. Choose the alert that you want to delete by choosing the alert information in the table.
3. Choose **Delete**.

A message displays asking you to confirm the deletion.

4. Click **Yes**.

The alert is removed from the dialog box.

Export Configuration Report

Use this option to save an ASCII file of all currently saved configuration data in Switch NV_RAM to your hard drive or a diskette. Use any desktop publishing application to import this ASCII file for viewing or printing.

NOTE: This file cannot be used to set configuration parameters through the Product Manager.

Data in the file includes:

- Product identification
Data input into the **Configure Identification** dialog box.
- Operating parameters
Data input into the **Operating Parameters** dialog box.
- Port parameters
Data input into the **Configure Ports** dialog box.

- SNMP parameters
Data input into the **Configure SNMP** dialog box.
- Active zoning configuration
This specifies the active zone and zone members, if set, and whether the default zone is enabled or disabled.

Procedure

To export a configuration report:

1. Choose **Export Configuration Report** from the **Configure** menu on the menu bar.

The **Export Configuration Report** dialog box displays.

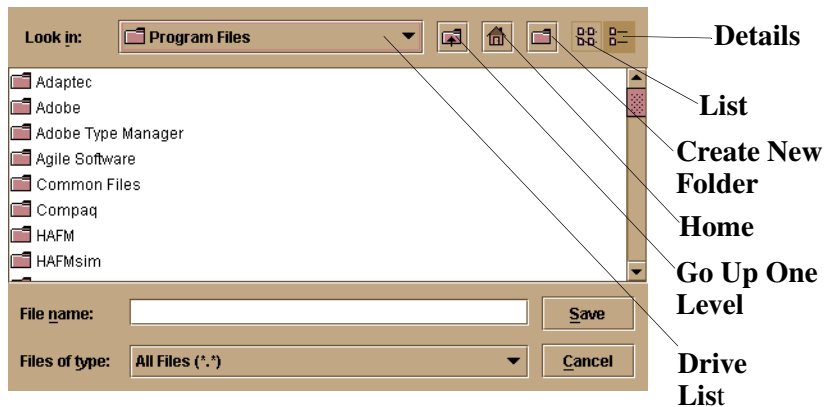


Figure 3–20: Export Configuration dialog box

2. Choose the folder where you want to save the file.
3. Type in a file name and extension in the **File name** field.
4. Click **Save**.

The file saves to the specified folder as an ASCII text file.

Enable Web Server

Choose this option from the **Configure** menu on the menu bar to place a check mark in the check box to enable the Embedded Web Server interface on the Switch. Choose the option again to remove the check mark and disable the Embedded Web Server interface. When enabled, users at remote workstations cannot access the interface. If enabled, HP recommends changing the user names and/or passwords from the default values to prevent unauthorized access.

Enable Telnet

Choose this option from the **Configure** menu on the menu bar to place a check mark in the check box to enable telnet access to the Switch. Choose the option again to remove the check mark and disable telnet access. When disabled, users at remote workstations cannot access the Switch through telnet to use the Command Line Interface (CLI) or perform other tasks. When enabled, users at remote workstations cannot access the interface. If enabled, HP recommends changing the user names and/or passwords from the default values to prevent unauthorized access.

Backing Up and Restoring Configuration Data

You can back up the NVRAM configuration, which includes all of the data you input through instructions in this chapter, using the **Backup and Restore Configuration** option. This option is available through the **Maintenance** menu. Choosing this option backs up the configuration data to a file on the HAFM server hard drive. The restore function writes this data back to NVRAM on the Switch. Using the restore function overwrites the existing configuration. For more information, refer to [Backup and Restore Configuration on page 5-7](#).

In addition to the **Backup and Restore Configuration** option, the Iomega *QuikSync* application backs up configuration and other critical data from the HAFM server automatically. As long as a Zip disk remains in the Zip drive of the HAFM server, data backs up to the Zip disk whenever the directory contents change or you reboot the HAFM server. For more information, refer to [Backup and Restore Configuration on page 5-7](#).

NOTE: We do not recommend changing the default QuikSync settings.

Using Logs

This chapter describes the Edge Switch 2/32 logs that you can access through the **Logs** menu on the **Product Manager** menu bar.

Using Logs

The Audit, Event, Hardware, Link Incident, and Threshold Alert logs store up to 1000 entries each. The most recent entry displays at the top of the log. After 1000 entries are stored, new entries overwrite the oldest entries.

Button Function

Button function is the same for all logs:

- **Clear** — Clicking **Clear** clears all entries in the log for all users. A warning dialog box displays requesting confirmation that you want to clear all entries in the log.
- **Refresh** — Clicking **Refresh** reads the current data and refreshes the screen with the new display.
- **Close** — Closes the log and displays the Switch **Product Manager** window.
- **Export** — Clicking **Export** on a log window displays the **Save** dialog box shown in [Figure 4-1 on page 4-2](#). Click the **Home** icon to return to the files in your home directory. The folders that list in the display area of the **Save** dialog box after clicking the **Home** icon, are those that are stored in your home directory. If you choose, you may create a folder for your home directory and save the file there.

To save a log file in American Standard Code for Information Exchange (ASCII) format to a location on your system's hard drive or to a diskette, use the following steps. You can open this file in any desktop publisher for viewing or printing.

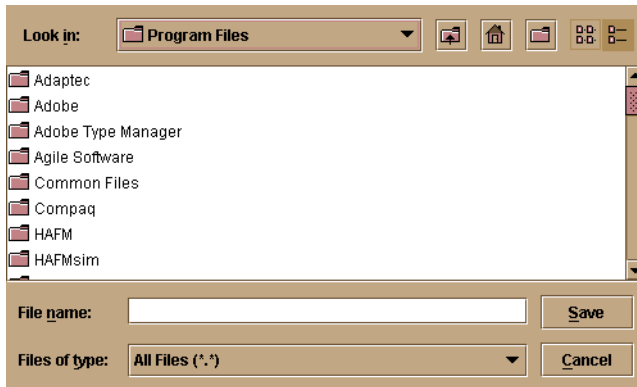


Figure 4-1: Save dialog box

1. Click **Export** on the log window.
The **Save** dialog box displays ([Figure 4-1](#)).
2. In the **Save** dialog box, choose the folder where you want to save the file.
3. Type in a file name and extension in the **File name** field.
4. Click **Save**.

The file saves to the specified folder as an ASCII text file.

Expanding Columns

Expand columns in logs by placing the cursor over the line separating column headings until a double arrow displays, then click and drag to widen the column as necessary.

Sorting Entries

Sort log entries in columns by clicking a column heading. A down arrow displays in the heading, if sorting alphabetically in descending order. An up arrow indicates sorting in ascending order. Click once to sort. Click again to reverse the sort.

Audit Log

The audit log displays a history of all configuration changes applied to the Switch from any source such as Product Manager, SNMP management stations, web server interface, host, or another Switch.

Date/Time	Action	Source	Identifier
10/3/01 9:44:53 AM(HAFM)	Operating Mode modified	HAFM	@172.18.3.24
10/3/01 9:44:53 AM(HAFM)	Operating Mode modified	HAFM	@172.18.3.24
10/3/01 9:44:53 AM(HAFM)	Interop Mode changed	HAFM	@172.18.3.24
10/3/01 9:44:53 AM(HAFM)	Operating Mode modified	HAFM	@172.18.3.24

Export... Clear Refresh Close

Figure 4–2: Audit Log

- **Date/Time** — The date and time of the change on the Switch.
Some actions, such as backing up configuration data and enabling automatic date/time synchronization, are performed only by the HAFM server without Switch interaction. These actions are indicated by the string, (HAFM), following the audit log's stamp of the HAFM server's date and time (refer to [Figure 4–2](#)). If the string, (HAFM), is not displayed, the time stamp is from the Switch.
- **Action** — User action that caused the configuration change, such as offline status, port name change, or change of address.

- **Source** — Identifies the user making the change through the Switch Product Manager and IP or DNS host name address of the remote user's workstation.
 - **Maintenance Port** — Change was made by a user connected to the maintenance port.
 - **HAFM** — Change was made by an Product Manager user.
 - **SNMP** — Change was made by a remote SNMP management station.
 - **Fabric** — Change was initiated by another Switch in the fabric that is not managed by this HAFM server.
 - **Web Server** — Change was made by a user through the Embedded Web Server Interface.
 - **Fibre Channel Host** — Change was made inband by a Fibre Channel host through the Open Systems Management Server or FICON Management Server.
 - **Telnet** — Change was made through a telnet connection.
- **Identifier** — Identifies the user making the change according to the source:
 - **Maintenance Port** — No entry displays.
 - **HAFM** — Includes user@address, where “user” is the Product Manager user name and “address” is the network address of the workstation (remote user workstation or HAFM server).
 - **SNMP** — Contains the network address of the SNMP management station.
 - **Fabric** — No entry displays.
 - **Web Server** — The Identifier column contains user@address, where “user” is the web server user name and “address” is the network address of the web user.
 - **Fibre Channel Host** — No entry displays.
 - **Telnet** — Change was made through a telnet connection.

Event Log

The event log provides a record of significant events that have occurred on the Switch, such as hardware failures, degraded operation, and port problems.

Date/Time	Event	Description	Severity	FRU-Position	Event Data
3/11/02 11:18:18 AM	070	E_Port has become segmented.	Informational		2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:15:54 AM	070	E_Port has become segmented.	Informational		2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:13:15 AM	203	Power supply AC voltage recovery.	Informational	PWR-0	

Export...
Clear
Refresh
Close

Figure 4–3: Event Log

All detected firmware faults and hardware failures are sent to the HAFM server for recording in the event log. The log provides a maximum of 1000 log entries before it wraps and overwrites the oldest entries.

For detailed information on event data and problem resolution, refer to the *hp StorageWorks edge switch 2/32 service manual (A7283-96002/AA-RS2GA-TE)*.

Each log entry includes the following:

- **Date/Time** — The date and time of the event on the Switch.
- **Event** — Events are identified by a unique code.

Event codes include:

000 - 199	System events
200 - 299	Power supply events
300 - 399	Fan module events
400 - 499	CTP events
500 - 599	Port events

- **Description** — A short description of the event.
- **Severity** — There are four classifications of severity that identify the importance of the event.
 - **Informational**
 - **Minor**
 - **Major**
 - **Severe**

- **FRU Position** — The FRU involved in the event and the slot position in the chassis relative to identical FRUs installed.
- **Event Data** — Up to 32 bytes of supplementary information for the event in hexadecimal format. For detailed information on event data and problem resolution, refer to the *hp StorageWorks edge switch 2/32 service manual (A7283-96002/AA-RS2GA-TE)*

Hardware Log

The hardware log displays information on field replaceable units (FRUs) inserted and removed from the Switch.

Date/Time	FRU	Position	Action	Part Number	Serial Number
2/14/02 9:09:18 AM	GSF2	1	Inserted	470-000396-201	121234561
2/14/02 9:09:18 AM	GSF2	0	Inserted	470-000396-201	121234560
2/14/02 9:09:18 AM	GXXL	13	Removed	470-000396-222	1012345613
2/14/02 9:09:18 AM	GSML	12	Removed	470-000396-201	912345612
2/14/02 9:09:18 AM	GLSL	11	Removed	470-000396-201	812345611
2/14/02 9:09:18 AM	GXXR	10	Removed	470-000396-201	1512345610
2/14/02 9:09:18 AM	GSMR	9	Removed	470-000396-201	141234569
2/14/02 9:09:18 AM	GLSR	8	Removed	470-000396-201	131234568
2/14/02 9:09:18 AM	GLSR	7	Removed	470-000396-222	131234567
2/14/02 9:09:18 AM	GLSR	6	Removed	470-000396-222	131234566

Export... Clear Refresh Close

Figure 4–4: Hardware Log

Each log entry includes the following:

- **Date/Time** — Date and time of the insertion or removal of the FRU.
- **FRU** — The name of the inserted or removed FRU.

FAN	Fan module
PWR	Power supply module
SFP	SFP transceiver.
CTP	CTP card. Note that the CTP card is not a FRU. If it fails, the Switch must be replaced.
- **Position** — Slot position in the chassis relative to identical components installed.
- **Action** — Inserted or removed.
- **Part Number** — Part number of the component.
- **Serial Number** — Serial number of the component.

Link Incident Log

The link incident log displays a thousand of the most recent link incidents with the date each incident occurred, the time it occurred, and the port where it took place.

Date/Time	Port	Link Incident
3/31/02 12:21:56 PM	23	Loss-of-Signal or Loss-of-Synchronization.
3/22/02 4:09:11 PM	23	Not Operational primitive sequence (NOS) received.
3/22/02 4:09:11 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 4:07:38 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 4:07:10 PM	3	Loss-of-Signal or Loss-of-Synchronization.
3/22/02 3:06:09 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 3:06:09 PM	23	Not Operational primitive sequence (NOS) received.
3/21/02 4:34:52 PM	3	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:30:11 PM	7	Not Operational primitive sequence (NOS) received.
3/21/02 4:29:13 PM	7	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:19:41 PM	3	Not Operational primitive sequence (NOS) received.
3/21/02 3:47:51 PM	23	Not Operational primitive sequence (NOS) received.
3/21/02 10:28:38 AM	15	Not Operational primitive sequence (NOS) received.
3/21/02 10:28:28 AM	23	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 10:27:03 AM	15	Loss-of-Signal or Loss-of-Synchronization.

Figure 4–5: Link Incident Log

Each log entry contains:

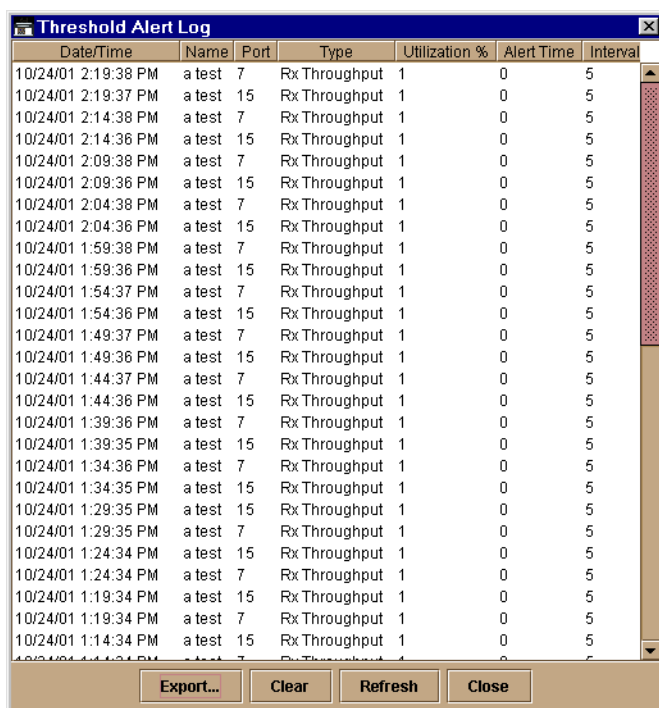
- **Date/Time** — The date and time of the incident.
- **Port** — The number of the port on which the incident occurred.
- **Link Incident** — A short description of the incident. The following events may cause a link incident to be written to the log.
 - Implicit incident.
The attached node detects a condition that may cause problems on the link.
 - Bit-error threshold exceeded.
The number of code violation errors has exceeded threshold.
 - Loss-of-signal or loss-of-synchronization. This occurs if a cable is unplugged from an attached node.
Loss-of-signal occurs when a cable is unplugged from an attached node.
Loss-of-synchronization condition has persisted for longer than the resource allocation time out value (R_A_TOV).
 - Not-operational (NOS) primitive sequence received.
A NOS was recognized.

- Primitive sequence timeout.
 - Link reset protocol timeout occurred.
 - Timeout occurred for an appropriate response while in NOS receive state and after NOS is no longer recognized.
- Invalid primitive sequence received for the current link state.

Either a link reset or a link reset response primitive sequence was recognized while waiting for the offline sequence.

Threshold Alert Log

This log provides details of threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Configure Threshold Alert(s)** option under the **Configure** menu.



Date/Time	Name	Port	Type	Utilization %	Alert Time	Interval
10/24/01 2:19:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:19:37 PM	a test	15	Rx Throughput	1	0	5
10/24/01 2:14:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:14:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 2:09:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:09:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 2:04:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:04:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:59:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:59:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:54:37 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:54:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:49:37 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:49:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:44:37 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:44:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:39:36 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:39:35 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:34:36 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:34:35 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:29:35 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:29:35 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:24:34 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:24:34 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:19:34 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:19:34 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:14:34 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:14:34 PM	a test	7	Rx Throughput	1	0	5

Buttons: Export... Clear Refresh Close

Figure 4-6: Threshold Alert Log

- **Date/Time** — Date and time stamp for when the alert occurred.
- **Name** — Name for the alert as configured through the **Configure Threshold Alerts** dialog box.
- **Port** — Port number where the alert occurred.
- **Type** — The type of alert: transmit (Tx) or receive (Rx).
- **Utilization %** — Percent usage of traffic capacity. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value and is configured through the **Configure Threshold Alerts** dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25 percent of the port's capacity.
- **Alert Time** — The maximum cumulative time that the throughput threshold percentage must exist before an alert is generated.
- **Interval** — The time interval during which the throughput is measured and an alert can generate. This is set through the **Configure Threshold Alerts** dialog box.

Using Maintenance Features

This chapter describes how to use the options that display from the **Maintenance** menu on the Product Manager menu bar.

Run Port Diagnostics

The **Port Diagnostics** option enables you to run internal and external loopback tests on any port. To use this option, follow the detailed steps in the *hp StorageWorks edge switch 2/32 service manual*.

Swap Ports

S/390 mode only. Choose **Swap Ports** to display the **Swap Ports** dialog box. Use this dialog box to swap one port address for another. For example, if the current address for port 0 is currently 04 and the address for port 1 is currently 05, you can swap so that the address for port 0 has address 05 and port 1 has address 04.

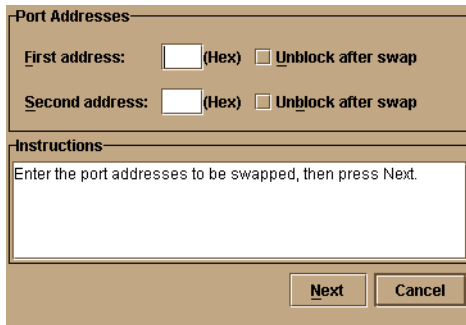
Make sure that the system administrator varies attached devices offline that are attached to the ports whose addresses you are going to swap. Ports that you are going to swap are blocked during this procedure, as swapping ports is disruptive to port operation.

Procedure

To swap ports, use the following steps:

1. Choose **Swap Ports** from the **Maintenance** menu on the menu bar.

The **Swap Ports** dialog box displays.



The image shows a 'Swap Ports' dialog box with a tan background. It has two sections: 'Port Addresses' and 'Instructions'. The 'Port Addresses' section contains two rows, each with a text input field labeled '(Hex)', a checkbox labeled 'Unblock after swap', and a label ('First address:' and 'Second address:'). The 'Instructions' section contains a text area with the text 'Enter the port addresses to be swapped, then press Next.' At the bottom right are 'Next' and 'Cancel' buttons.

Figure 5–1: Swap Ports dialog box

2. Enter the first address (in hexadecimal format).
3. If you want to unblock the port, click **Unblock after swap**. Note that ports are automatically blocked during the swap process.
4. Enter the second address (in hexadecimal format).
5. If you want to unblock the port, click **Unblock after swap**.
6. Click **Next** to continue.
7. Follow the on-screen instructions and click **Next** to continue through to the next screen.
8. If you are finished configuring the Switch, back up the configuration data. For more information, refer to [Backup and Restore Configuration on page 5-7](#).

Collect Maintenance Data

The **Data Collect** option enables you to collect maintenance data that can help support personnel diagnose system problems. Save this data to a zip file on a Zip disk (or other medium with the appropriate capacity), and forward it to technical support personnel.

Execute an IPL

To use this option, follow the detailed steps in the *hp StorageWorks edge switch 2/32 service manual* **Execute an IPL**



CAUTION: The Ethernet connection between the HAFM server and Switch is interrupted momentarily during an IPL.



CAUTION: An initial program load (IPL) is not intended for ordinary or casual use and should only be performed if the control processor (CTP) card is suspected to be faulty. Do not use this option unless directed by your support representative or if you need to reset a failed CTP card. An IPL will disrupt port operations. Before using this option, make sure administrators of device(s) attached to ports quiesce Fibre Channel traffic through the Switch and take the device offline. Note that the CTP card is not a FRU. If it fails, the Switch must be replaced.

If it is necessary for you to execute an IPL on the Switch, use the following steps:

1. Choose **IPL** from the **Maintenance** menu on the menu bar.

A dialog box displays confirming the IPL.

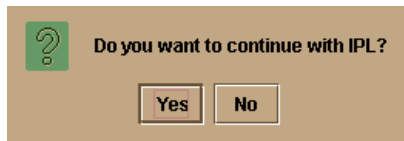


Figure 5–2: IPL Confirmation dialog box

2. Click **Yes**.

Choosing **IPL** from the **Maintenance** menu causes Ethernet connection between the Switch and HAFM server to drop momentarily and the following to occur in the Product Manager window:

- As the network connection drops, the Switch **Status** table on the **Hardware** view turns yellow.
- The **Status** field in the table displays “No Link” and the **State** field displays the reason for no link.
- A grey square displays in the status bar. Refer to [Table 1–1 on page 1-32](#) for an explanation of this status bar display.

- The FRUs illustrated in the **Hardware** view do not display. They display again as the connection is re-established.

An IPL initiates the following functions in the Switch:

- Restarts the operational firmware on the CTP card, executes abbreviated power on system tests (POSTs) and then, if no POST errors are encountered, the Switch resumes the active role that it had before the IPL. Note that the CTP card is an internal component and is not a FRU.
- Resets the Ethernet interface on the CTP card, causing the connection to the HAFM server to drop momentarily. The status symbol for the Switch in the Product view will change to a gray square until the connection is reestablished.
- Stops normal switching functions for ports (functions resume after the IPL).

After the IPL:

- All Fabric services databases containing information about current Fabric logins, name server registrations, and other data remain intact, making the operation transparent to attached devices.
- The Switch returns to the online state, even if it was offline before the operation.
- All ports configured as blocked will remain blocked.
- Modifications made to an active zone set configuration that have not been enabled will be automatically enabled.

Set Online State

Use the procedure in this section to display the current Switch operating state (offline or online) and change the state as required.



CAUTION: Before setting the Switch offline, warn administrators and users currently operating devices that are attached to the Switch that it is going offline and that there will be a disruption of communications. Make sure administrators of device(s) attached to ports quiesce Fibre Channel traffic through the Switch.

To set the Switch online or offline (depending on current state), use the following steps:

1. Right-click the Switch in the **Hardware** view and choose **Set Online State** in the menu, or choose **Set Online State** from the **Maintenance** menu on the menu bar.

One of the following dialog boxes displays, depending on the current operating state.

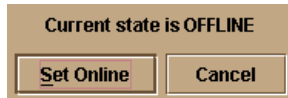


Figure 5-3: Set Online State dialog box (Offline)

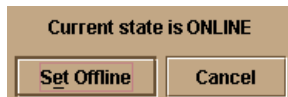


Figure 5-4: Set Online State dialog box (Online)

2. Click **Set Offline** or **Set Online**, depending on the operating state you want to set.
3. When a warning box displays requesting you to confirm the offline or online state, click **OK**.

As the Switch goes offline, “OFFLINE” displays in the **State** field of the **Switch Status** table in the **Hardware** view. LED indicators on all ports with attached devices stay green, but the Switch is sending offline sequences (OLSs) to these devices.

Manage Firmware Versions

Firmware refers to the internal operating code for the Switch. You can maintain up to eight firmware versions on the HAFM server for downloading to an Switch. To use the **Firmware Library** option to manage firmware versions, follow the steps in the *hp StorageWorks edge switch 2/32 service manual*.

Enable E-Mail Notification

E-mail addresses and the simple mail transfer protocol (SMTP) server address for e-mail notification of Switch events must be configured through the *HAFM* application. Refer to the *hp StorageWorks ha-fabric manager user guide* for instructions on configuring e-mail.

NOTE: E-mail recipients are configured in the HAFM through the **Configure E-Mail** dialog box. A valid SMTP address is configured in this dialog box.

Use the **Enable E-Mail Notification** function on the Product Manager to enable e-mail notification for events that occur on a selected Switch. The default state is disabled.

To enable e-mail notification, use the following steps:

1. Choose **Enable E-Mail Notification** from the **Maintenance** menu on the menu bar.
2. To enable e-mail notification, choose the option to add a check mark to the check box.
3. To disable e-mail notification, choose the option to remove the check mark from the check box.

Enable Call-Home Notification

The call-home feature enables the HAFM server to automatically dial out to a support center to report system problems. The support center server accepts calls from the HAFM server, logs reported events, and notifies one or more support center representatives.

You must enable Call-Home Event Notification through the StorageWorks *HAFM* application Maintenance Menu before enabling this function through the Product Manager for individual Directors. Two call-home options are available but only one can be used when HAFM is installed:

- In legacy Hewlett-Packard environments, call-home notification for Directors and Switch requires installation of Proactive Service software. This service is offered at no additional charge for subsystems covered under an on-site warranty or on-site storage hardware support contract. To register or order Proactive Services software, contact your HP customer service representative.

- In classic HP environments, configure telephone numbers and other information for the call-home feature through the Windows dial-up networking application. Refer to the *hp StorageWorks HAFM server installation guide* for details.

Use the **Enable Call Home Notification** function on the Product Manager to enable call-home notification for events that occur on the selected Switch. The default state is disabled.

To enable call-home notification for system problems, use the following steps:

1. Choose **Enable Call Home Notification** from the **Maintenance** menu on the menu bar to enable and disable call-home notification.

A check mark displays next to the menu option to indicate that call-home notification is enabled.

2. Click the check box to add or remove the check mark.

Backup and Restore Configuration

Choose this option from **Maintenance** menu to save the product configuration stored on the Switch to the HAFM server hard disk or to restore the product configuration from the HAFM server. Only a single copy of the configuration is kept on the server.

The purpose of the backup is primarily for restoring configuration data to a replacement Switch. You can also use this feature for a special purpose configuration or for temporary testing of a configuration. You cannot modify the location and file name of the saved configuration.

NOTE: You can only restore the configuration to a Switch with the same IP address.

Backup

1. Choose **Backup and Restore Configuration** from the **Maintenance** menu on the menu bar to display the **Backup and Restore Configuration** dialog box.

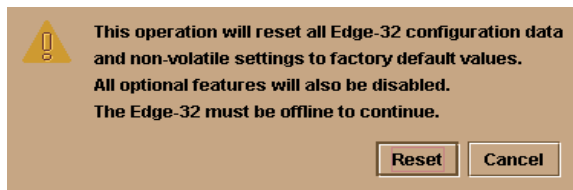


Figure 5–5: Backup and Restore dialog box

The **Backup and Restore** dialog box consists of a short description of the features performed when you choose **Backup** or **Restore**.

Following is a list of configurations that are backed up to the HAFM server:

- Identification data (Switch name, description, and location).
 - Port configuration data (port names, blocked states, and extended distance settings).
 - Operating parameters (BB_Credit, E_D_TOV, R_A_TOV, Switch priority, preferred domain ID, and rerouting delay).
 - SNMP configuration (trap recipients, community names, and write authorizations).
 - Zoning configuration (active zone set and default zone state).
2. To backup data, click **Backup**.
 3. When the dialog box displays confirming that the backup of configuration is complete, click **OK**.

If the backup fails, a dialog box displays to inform you that the backup to the server failed.

Restore

1. Set the Switch offline before performing the restore function.
2. Click **Restore** on the **Backup and Restore Configuration** dialog box to restore the backed up configuration to the nonvolatile random access memory (NVRAM) on the Switch.

Set the Switch to offline before performing the restore function. If you choose **Restore** and the Switch is online, a message dialog displays requesting that you turn the Switch offline. No action takes place when you close the dialog box. For instructions on setting the Switch offline or online, refer to [Set Online State on page 5-4](#).

If the Switch is already offline and you click **Restore**, a confirmation dialog box displays indicating that the restore will overwrite any existing configuration already on the Switch. The dialog box also displays the date of the restored backup. Click **OK**.

Note that the restore operation initiates an IPL.

3. Set the Switch back online when the restore completes.

Reset Configuration

NOTE: You must have maintenance authorization rights to access this feature.

This option resets all configuration data input through options in the **Configure** menu, zoning configurations, and Switch addressing to factory-default values. Since the current IP address for the Switch may not match the factory default address, the Ethernet link between the Switch and the service processor may drop and not reset. Before using this option, record the Switch's current IP address which displays below the Switch's icon in the HAFM's **Product** view (view **Display Options** set to **Network Address**). You can also find the current IP address through the Embedded Web Server Interface.

After resetting the configuration, you must reset the original address on the Switch through the maintenance port or the Embedded Web Server Interface to maintain LAN connections and communication with the service processor.

Procedure

1. Set the Switch offline. For instructions, refer to [Set Online State on page 5-4](#).
2. Choose **Reset Configuration** from the **Maintenance** menu on the menu bar. The following warning displays:



WARNING: This operation will reset all Switch configuration data and non-volatile settings to factory default values. All optional features will also be disabled. The Switch must be offline to continue.

NOTE: If you have enabled features that add additional port function since the Switch was shipped from the factory, these features will be disabled (factory default) when the configuration is reset. Only those ports that were enabled at the factory will function. You will have to enable the additional port function features again through the [Configure Feature Key dialog box](#).

Factory-default values may vary, depending on the firmware release installed in your Switch. For a list of values, refer to the *hp StorageWorks edge switch 2/32 service manual*.

Optional Features

This chapter provides detailed information on using, administering, and configuring optional HAFM features through HAFM applications. There are two types of features covered in this chapter:

- “Keyed” features, requiring feature keys to be purchased and enabled through the **Configure Feature Key** dialog box in the product’s *Product Manager* application.
- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through *HAFM* or *Product Manager* applications.

FICON Management Server

The FICON Management Server is a keyed feature that allows host control and inband management of the Director or Switch through an IBM System/390 or zSeries 900 Parallel Enterprise Server server attached to a Director or Switch port. The server communicates with the Switch or Director through a FICON channel. Control of connectivity and statistical product monitoring are provided through a host-attached console.

Installation

To install and enable this option, choose the **Configure Feature Key** option under the Product Manager’s **Configure** menu.

Configuring the FICON Management Server

Use this procedure to configure whether the host is the controlling manager.

The optional FICON Management Server feature must be installed in order to perform this procedure.

- **Enable Management Server**

Click this check box to add a check mark and enable the management server.

Click the check mark to remove it and disable this feature.

- **Switch Clock Alert Mode**

Click this check box to display a check mark and enable clock alert mode. If this is enabled, the following occurs when users set the date and time through the

Configure Date and Time dialog box (**Configure** menu):

- If you enable **Periodic Date/Time Synchronization**, an error message displays indicating that Clock Alert Mode must be cleared to enable automatic synchronization of the date and time.
- If you manually set the date and time (**Periodic Date/Time Synchronization** is not enabled), a confirmation dialog box will display. You must click **OK** on that dialog box to continue manual configuration.

- **Host Control Prohibited**

Click this check box to display a check mark and prohibit a host management program from changing configuration and connectivity parameters on the Switch. In this case, the host program will have read authorization only and cannot make changes. When the check mark is not displayed, a host program can change configuration and connectivity parameters on the Switch.

- **Programmed offline state control**

Click this check box to display a check mark and enable a host management program to control the Switch's offline and online state. When a check mark is not displayed, a host program cannot set the Switch online or offline.

- **Active=Saved**

Click this check box to display a check mark and enable the **active=saved** function for the IPL address configuration.

- If **Active=Saved** is enabled (check mark), the IPL and the active address configuration are maintained as identical configurations. If a new configuration is activated through the **Configure Addresses - "Active"** dialog box, that configuration becomes the IPL address configuration.

- If **Active=Saved** is not enabled (no check mark), the IPL address configuration and the active configuration are not maintained as identical, and may be different configurations. If the feature *is not* enabled, you can modify the IPL configuration through the **Configure Addresses - “Active”** dialog box. If the feature *is* enabled, the IPL file is locked to modification through the **Configure Addresses - “Active”** dialog box.

- **Code Page**

Consider the language required for the port name display that displays on the HAFM Server. Language support is provided through character set 697 for all Extended Binary-Coded Decimal Interchange Code (EBCDIC) pages.

When planning the installation, choose the EBCDIC code page for displaying host-assigned port names or the CUP name. As an example, if the code page for Italy is selected and a port name is assigned in Italian by the host management program, then the Italian language port name will display in the Product Manager.

This field lists the code pages that are available for configuration. The default code page is United States/Canada 00037. Refer to the following table for other code pages:

Table 6–1: Available Code Pages

Code Page Name	Code Page	Hexadecimal CPGID
United States/Canada	00037	0025
Germany/Austria	00273	0111
Brazil	00275	0113
Italy	00280	0118
Japan	00281	0119
Spain/Latin America	00284	011C
United Kingdom	00285	011D
France	00297	0129
International #5	00500	01F4

Procedure

To configure the FICON management server, use the following steps:

1. Choose **Configure > Management Server** from the **Product Manager** window. The **Configure FICON Management Server** dialog box displays, as shown in [Figure 6–1](#).



Figure 6–1: Configure FICON Management Server dialog box

2. Enable or disable the management server by clicking **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)
3. Enable or disable Switch clock alert mode by clicking the **Director Clock Alert Mode** check box. When a check mark displays, the alert mode is enabled.
4. Allow or prohibit host control by clicking the check box in the **Host Control Prohibited** field. When a check mark displays, host control is prohibited.
5. Allow or prohibit offline state control by clicking the check box in the **Programmed offline state control** field. When a check mark displays, programmed control of the offline state is allowed.
6. Enable or disable Active=Saved mode by clicking the check box in the **Active=Saved** field. When a check mark displays, the Active=Saved mode is enabled.
7. If necessary, choose a code page from the **Code Page** drop-down list.
8. Activate changes and close the dialog box by clicking the **Activate** button.
9. If you are finished configuring the Switch, back up the configuration data.

Open Systems Management Server

The Open System Management Server (OSMS) is a keyed feature that allows host control and inband management of the Director or Switch through a management application that resides on an open-systems interconnection (OSI) device. This device is attached to a Director or Switch port. The device communicates with the Switch or Director through Fibre Channel common transport (FC-CT) protocol.

Installation

To install and enable this option, choose the **Configure Feature Key** option under the Product Manager's **Configure** menu.

Configuring the Open Systems Management Server

Use these procedures to configure the open systems inband management program to function with the Switch.

The optional Open Systems Management Server feature must be installed in order to perform this procedure.

Procedure

To configure open systems management server, use the following steps:

1. Choose **Configure > Management Server** from the **Product Manager** window. The **Configure Open Systems Management Server** dialog box displays, as shown in [Figure 6–2](#).

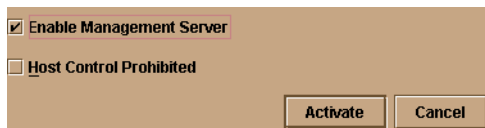


Figure 6–2: Configure Open Systems Management Server dialog box

2. Enable the management server by clicking the **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)

3. Click the check box in the **Host Control Prohibited** field to display a check mark and to prohibit the host management program from changing configuration and connectivity parameters on the Switch. In this case, the host program has read-only access to configuration and connectivity parameters. Clicking the check box when it contains a check mark removes the check mark and allows a host program to change configuration and connectivity parameters on the Switch.
4. To activate changes and close the dialog box, click **Activate**.
5. If you are finished configuring the Switch, you can back up the configuration data.

SANtegrity Features

SANtegrity includes a set of features that enhance security in SANs (Storage Area Networks) that contain a large and mixed group of fabrics and attached devices. Through these features you can allow or prohibit Switch attachment to fabrics and device attachment to Switches. These features are enabled by purchasing a feature key, then enabling the key through the **Configure Feature Key** dialog box.

SANtegrity features include:

- Fabric Binding
- Switch Binding

Enterprise Fabric Mode - Although this is not a keyed feature, the SANtegrity Fabric Binding and Switch Binding must be installed before you can use Enterprise Fabric Mode function through the **HAFM Fabrics** menu.

Fabric Binding

This feature is managed through the **Fabric Binding** option, available through the **Fabrics** menu in HAFM when the **Fabrics** tab is selected. Using Fabric Binding, you can allow specific Switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Enable/Disable and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the Director or Switch is offline or online. Be aware of the following:

- Because Switches are bound to a fabric by World Wide Name (WWN) and domain ID, the Insistent Domain ID option in the **Configure Switch Parameters** dialog box is automatically enabled if Fabric Binding is enabled. You cannot disable Insistent Domain ID while Fabric Binding is active and the Switch is online.
- If Fabric Binding is enabled and the Switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the Director or Switch is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

Switch Binding

This feature is managed through the **Switch Binding** submenu options available on the Product Manager **Configure** menu. Using **Switch Binding**, you can specify devices and Switches that can attach to Director and Switch ports. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a Switch or Director.

Configuring Switch Binding - Overview

To configure Switch binding, you must first activate the feature using the **Switch Binding State Change** dialog box while choosing the type of port where you want to restrict connection (connection policy). Possible selections are **E_Ports**, **F_Ports**, or **all types**.

If the Director or Switch is online, activating Switch binding populates the Membership List in the **Switch Binding - Membership List** dialog box (Product Manager) with the following WWNs currently connected to the Director or Switch, depending on the connection policy set in the **State Change** dialog box:

- WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.

- WWNs of Switches connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached Switch.
- WWNs of devices connected to F_Ports and Switches connected to E_Ports (all-ports connection policy).

Notes

- When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, Switches, or both that are currently connected to the Switch.
- If the Switch is offline and you activate Switch binding, the Membership List is not automatically populated.
- Edits to the Switch Binding Membership list will be maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and/or Switches from connecting with Director or Switch ports by removing them from the Membership List in the **Switch Binding Membership List** dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and Switches.

Enable/Disable Switch Binding

1. Choose the **Configure > Switch Binding > Change State** from the **Product Manager** window. The **Switch Binding State Change** dialog box displays, as shown in [Figure 6–3](#).

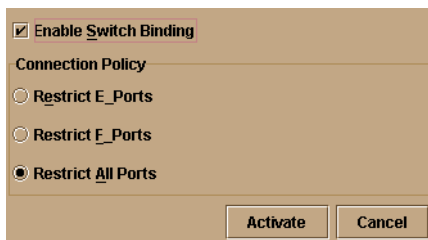


Figure 6–3: Switch Binding State Change dialog box

2. Perform one of the following steps:
 - To disable Switch Binding (a check mark displays in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to remove the check mark, then click **Activate**.
 - To enable Switch Binding (check mark is not in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to add a check mark. Go on to step 3 to set the Connection Policy.
3. Click one of the **Connection Policy** options.
 - **Restrict E_Ports**. Choose if you want to restrict connections from specific Switches to Switch E_Ports. Switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.
 - **Restrict F_Ports**. Choose if you want to restrict connections from specific devices to Switch F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Switches are allowed to connect to any E_Port.
 - **Restrict All**. Choose if you want to restrict connections from specific devices to Switch F_Ports and Switches to Switch E_Ports. Device and Switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection.
4. Click **Activate** to enable the changes and close the dialog box.
5. Edit the Switch Membership List through the **Switch Binding Membership List** dialog box to add or remove Switches and devices that are allowed to connect with the Switch.

Editing the Switch Membership List

1. Choose the **Configure > Switch Binding > Edit Membership List** from the **Product Manager** window. The **Switch Binding Membership List** dialog box displays, as shown in [Figure 6-4](#).

The WWNs of devices and/or Switches that can currently connect to Switch ports are listed in the **Switch Membership List** panel.

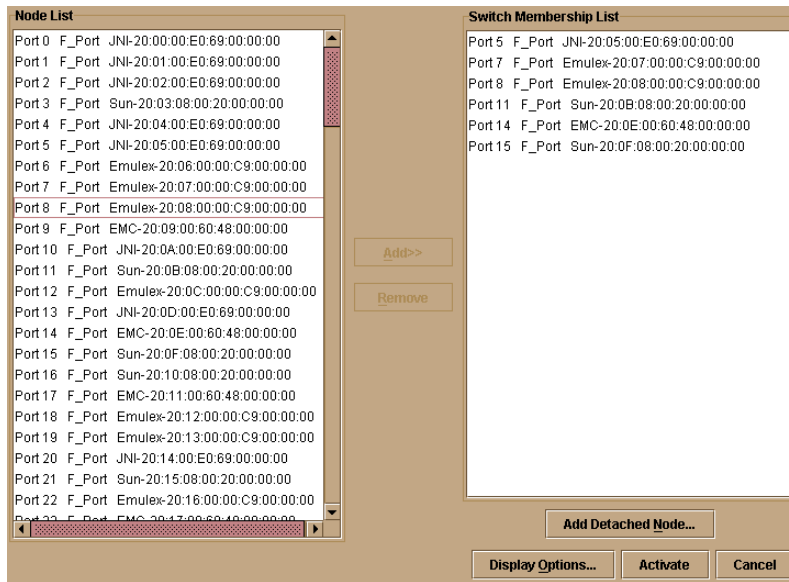


Figure 6-4: Switch Binding Membership List dialog box

Refer to [Configuring Switch Binding - Overview on page 6-7](#) for information on how the Switch Membership List is populated with WWNs according to options set in the **Switch Binding State Change** dialog box.

2. If nicknames are configured for WWNs through HAFM and you want these to display instead of WWNs in this dialog box, click **Display Options**. The **Display Options** dialog box displays.
3. Click **Nickname**, then click **OK**.
4. To prohibit connection to a Switch port from a WWN currently in the Membership List, click the WWN or nickname in the **Membership List**, then click **Remove**. The WWN or nickname will move to the **Node List** panel. WWNs can only be removed from the fabric if any of the following is true:
 - The Switch is offline.
 - Switch Binding is disabled.
 - The Switch or device with the WWN is not connected to the Switch.

- Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the **Switch Binding State Change** dialog box. For example, a WWN for a Switch attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to Restrict F_Ports.
 - The Switch or device with the WWN is connected to a port that is blocked.
5. The Switch or device with the WWN is not currently connected to the Switch (detached node).
 6. WWNs can be added to the **Switch Membership List** (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a Switch port from a WWN in the **Node List** panel, choose the WWN or nickname in the **Node List** panel, then click the **Add** button. The WWN or nickname will move to the **Membership List** panel.
 7. To add a WWN for a device or Switch not currently connected to the Switch, click **Detached Node**. The **Add Detached Node** dialog box displays.
 8. Enter the appropriate WWN or nickname (if configured through HAFM) and click **OK**. The WWN or nickname displays in the **Switch Membership List**.
 9. Click **Activate** to enable the changes and close the dialog box.

Enable/Disable and Online State Functions

In order for Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the Director or Switch is offline or online. Be aware of the following:

- Switch Binding can be enabled or disabled whether the Switch is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled.
- If Enterprise Fabric Mode is enabled and the Director or Switch is online, you cannot disable Switch Binding. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.
- If Enterprise Fabric Mode is enabled and the Director or Switch is offline you can disable Switch Binding, but Enterprise Fabric Mode will also disable.

- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.
- WWNs can only be removed from the Switch Membership List if any of the following are true:
 - The Director or Switch is offline.
 - Switch Binding is disabled.
 - The Switch or device with the WWN is not connected to the Director or Switch.
 - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the **Switch Binding State Change** dialog box. For example, a WWN for a Switch attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to Restrict F_Ports.
 - The Switch or device with the WWN is connected to a port that is blocked.
 - The Switch or device with the WWN is not currently connected to the Director or Switch (detached node).
- If the Director or Switch is online and Switch Binding is not enabled, all nodes and Switches attached to the Director or Switch are automatically added to the Switch Membership List.

Zoning with Switch Binding Enabled

Note that SANtegrity has no effect on existing zoning configurations. However, note that if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the device cannot log in to the Director or Switch port and cannot connect to other devices in the zone with Switch Binding enabled.

Enterprise Fabric Mode

Enterprise Fabric Mode is an option available on the **Fabrics** menu in the *HAFM* application if the SANtegrity feature key is installed. This option automatically enables the following features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. Note that there are specific requirements for disabling these parameters and features when the Director or Switch is offline or online.

Fabric Binding

This is a SANtegrity feature enabled through the **Fabrics** menu in HAFM that allows or prohibits Switches and Directors from merging with a selected fabric. Refer to [Enable/Disable and Online State Functions on page 6-7](#) for details on enabling/disabling Fabric Binding with Enterprise Fabric Mode.

Switch Binding

This is a SANtegrity feature enabled through the **Configure** menu in the Product Manager that allows or prohibits Switches and/or Directors from connecting to Switch E_Ports, devices from connecting to F_Ports. Refer to [Enable/Disable and Online State Functions on page 6-11](#) for details on enabling/disabling Switch Binding with Enterprise Fabric Mode enabled.

Rerouting Delay

Rerouting delay is a parameter in the **Configure Switch Parameters** dialog box, available from the **Configure** menu in the *Product Manager* application.

Rerouting Delay ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new Switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the E_D_TOV field of the **Configure Fabric Parameters** dialog box (**Configure** menu). This delay enables frames sent on the old path to exit to their destination before new frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless the Director or Switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode.

Domain RSCNs

This is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the *Product Manager* application. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the Director or Switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode.

Insistent Domain Identification (ID)

This is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the *Product Manager* application. Enabling this option sets the domain ID configured in the **Preferred Domain ID** field in the **Configure Switch Parameters** dialog box as the active domain identification when the fabric initializes. A static and unique domain identification is required by the Fabric Binding feature because the feature's Fabric Membership list identifies Switches by WWN and Domain ID. If a duplicate preferred domain ID is used, then insisted, warnings occur when Directors and Switches are added to a Fabric Membership List.

If Fabric Binding or Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless these options are disabled when the Director or Switch is offline. If the Director or Switch is online, disabling Insistent Domain ID will disable Enterprise Fabric Mode and Fabric Binding.

Product Manager Messages

This appendix lists and explains messages that may display in message boxes as you use the Product Manager. Solutions to problems implied by each message are included when applicable.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages

Message	Description	Action
Activating this configuration will overwrite the current configuration.	Confirmation to activate a new address configuration.	Click Yes to confirm activating the new address configuration or No to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All port names must be unique.	A duplicate port name was entered. Every configured port name must be unique.	Reconfigure the port with a unique name.
Another Product Manager is currently performing a firmware install.	Only one firmware install to a specific switch can take place at a time.	Wait for the current firmware install to complete and try again.
Are you sure you want to delete firmware version?	Requesting confirmation to delete the firmware version. Firmware library can hold only eight firmware versions.	Click Yes to confirm the firmware deletion or No to cancel the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click Yes to confirm the deletion of the address configuration or No to cancel the operation.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Are you sure you want to send firmware version?	Confirmation to add a firmware version to the firmware library. The firmware library can hold eight firmware versions.	Click Yes to confirm adding the firmware version to the firmware library, or no to cancel the operation.
Cannot change Port Type while in S/390 mode without SANtegrity feature. Please contact your sales representative.	User attempted to change a port type in the Configure Ports dialog box while in S/390 mode, but the optional SANtegrity feature is not installed.	Informational message. Install SANtegrity before changing port types in the Configure Ports dialog box while in S/390 operating mode.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	User attempted to disable switch binding through the Switch Binding Change State dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the <i>HAFM</i> application or set the Switch offline before you can disable Switch Binding.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Choose Clear System Error Light from Product menu to clear error light, then enable beaconing.
Cannot have E-Ports configured in S/390 mode Unless SANtegrity feature is installed. Please contact your sales representative.	User attempted to change operating mode from Open Systems to S/390 mode with E_Ports configured but SANtegrity is not installed.	Informational message. If you install SANtegrity before changing to S/390 mode, then E_Ports will remain as E_Ports when you change to S/390 mode. If SANtegrity is not installed, setting a Switch to S/390 mode will change all E_Ports to G_Ports.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Cannot have spaces in field.	Spaces are not allowed in this field.	Remove the spaces or retype the field without spaces.
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a Switch with a defective CTP card.	Note that the CTP card is not a FRU. If it fails, the Switch must be replaced. After replacement, retry the firmware install to the Switch.
Cannot perform this operation while the switch is offline.	This operation cannot take place while the Switch is offline.	Configure the Switch offline through the Set Online State dialog box then retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve diagnostics results.	Diagnostics results cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve information for port.	Information for the port cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port configuration.	Port configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port information.	Port information cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port statistics.	Port statistics cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve switch date and time.	Switch date and time cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Cannot retrieve switch state.	Switch state cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot run diagnostics on a port that is failed.	Port diagnostics cannot be performed on a port that has failed.	Run diagnostics only on an operational port.
Cannot run diagnostics on an active E-port.	Port diagnostics cannot be performed on an active E-port.	Run diagnostics on an E-port only when it is not active.
Cannot run diagnostics while a device is logged-in to the port.	A device is logged in to the port where a diagnostic test is attempted.	Log out the device and run the diagnostic test again.
Cannot run diagnostics. The port is not installed.	Port diagnostics cannot be performed when the port is not installed.	Run diagnostics only on a port that is installed.
Cannot save IPL configuration file while active=save is enabled.	The user cannot save the IPL file while the active=saved property is set.	The FICON management server property, active=saved, must be disabled for HAFM to save the IPL file.
Cannot save port configuration.	Port configuration cannot be saved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot save SNMP configuration.	SNMP configuration cannot be saved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set all ports to 1 Gb/sec due to port speed restriction on some ports.	Displays if you try to set ports to operate at 1 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Cannot set all ports to 2Gb/sec due to port speed restriction on some ports.	Displays if you try to set ports to operate at 2 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set Fibre Channel parameters.	Fibre Channel parameters cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set switch date and time.	Switch date and time cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set switch state.	Switch state cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set write authorization without defining a community name.	A community name was not defined in the Configure SNMP dialog box for the write authorization selected.	Provide a name in the name field where write authorization is checked.
Cannot start data collection.	Data collection cannot be started. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot start port diagnostics.	Port diagnostics cannot be started. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot swap an uninstalled port.	A port swap cannot be performed when the port is not installed.	Perform a swap only on a port that is installed.
Click OK to remove all contents from log.	Requesting confirmation that you want all contents removed from the log.	Click OK to continue or Cancel to cancel the operation.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Could not export log to file.	A file I/O error occurred. The log file could not be saved to the specified destination.	Ensure filename and drive are correct.
Could not find firmware file.	Firmware file selected was not found in the FTP directory.	Ensure file name and directory are correct.
Could not find firmware file.	The selected file is not a firmware file.	Obtain a valid firmware file from your service representative.
Could not remove dump files from server.	Dump files could not be removed from server. Link may be down or Switch may be busy.	Retry the operation later. If the condition persists, contact support personnel.
Could not stop port diagnostics.	Port diagnostics could not be stopped. Link may be down or Switch may be busy.	Retry the operation later. If the condition persists, contact support personnel.
Could not write firmware to flash.	Firmware could not be written to flash memory.	Try again. If problem persists, contact support personnel.
CUP name and port name are identical.	Within the address configuration, one or more of the port names are the same as the CUP name.	Make sure all names are unique for the ports and CUP name.
Date entered is invalid.	Date entered incorrectly.	Verify that the number of days in the month is valid.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Device application is not terminated.	Terminate device application before running port diagnostics.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	User attempted to remove a device WWN from the Switch Membership List (SANtegrity feature) while Switch Binding is enabled.	Remove the device from the Switch by blocking the port, setting the Switch offline, or disabling Switch Binding through the Switch Binding Change State dialog box before removing devices from the Switch Membership List.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue	Fabric Binding is enabled through HAFM and user attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box.	Click Yes if you want to continue and disable Fabric Binding.
Do you want to continue with IPL?	Requesting confirmation to proceed with an IPL.	Click Yes to confirm the IPL or Cancel to cancel the operation.
Duplicate community names require identical write authorizations.	Duplicate community names exist that have conflicting or different write authorizations.	Verify community names and whether a community name is duplicated with different write authorizations.
Enterprise Fabric Feature not installed. Please contact your sales representative.	The user selected Switch Binding from the Configure menu, but the optional SANtegrity feature is not installed.	Install the SANtegrity key through the Configure Feature Key dialog box before using Switch Binding features.
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCNs. Do you want to continue?	User attempted to disable these parameters in the Configure Switch Parameters dialog box while the Switch was online, but Enterprise Fabric Mode (SANtegrity feature) is enabled.	Click Yes if you want to continue, and disable Enterprise Fabric Mode.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Error retrieving port information.	An error occurred while retrieving port information. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error retrieving port statistics.	An error occurred while retrieving port statistics. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error stopping port diagnostics.	An error occurred while attempting to stop the port diagnostics from running. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error transferring files <message>.	An error occurred while attempting to download files.	Retry the operation. If the condition persists, contact support personnel.
Field cannot be blank.	A blank field is not allowed in this dialog.	Enter the required information in the blank field.
File transfer aborted.	User has stopped the file transfer.	N/A. An informational message.
File transfer is in progress.	Firmware or data collection is being transferred.	N/A. An informational message.
Firmware download timed out.	The Switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact support personnel.
Firmware file I/O error.	Firmware file input/output error occurred.	Contact support personnel.
Firmware file not found.	Firmware file deleted from the HAFM server.	Add firmware to library.
Incompatible configuration between operating mode and management server.	The user has selected the open systems operating mode, but has the FICON Management Server feature installed, and is attempting to activate the operating mode.	User needs to install Open Systems Management server or choose S/390 operating mode.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Incorrect product type.	When configuring a new product through the New Product dialog box, an incorrect product was selected for the network address.	Choose the correct product type for the product with the network address.
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the Switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM server will be lost momentarily, but Fibre Channel traffic will not be affected.	Click Yes to install the feature key or No to not install.
Internal file transfer error received from switch.	Switch detected an internal file transfer error.	Contact support personnel.
Invalid character in field.	Invalid character in the input field.	Re-enter the field information.
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens and underscores.
Invalid feature key.	The feature key was not recognized.	Re-enter the feature key noting the key is case sensitive and to include the dashes.
Invalid firmware file.	Selected file is not a firmware file.	Choose the correct firmware file.
Invalid network address.	Network address specified is not known by the domain name server.	Check the input address and specify the correct network address.
Invalid port address.	Invalid port address has been entered.	Verify port address through the Configure Addresses - "Active" dialog box (S/390 mode only) and re-enter.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Invalid port number.	Port number must be within the range of ports for the specific Switch model.	Enter a port number within the correct range.
Invalid port number. Valid ports are (0 - 31).	Port number must be within the range of ports for the specific Switch model. For this model, the valid port numbers are 0 - 31.	Enter a port number within the correct range.
Invalid port swap.	Port swap selection is not allowed.	Ensure that each port selected for swap has not been previously swapped.
Invalid response received from switch.	The Switch returned an invalid response.	Resend the firmware. If the condition persists, contact support personnel.
Invalid serial number for this feature key.	The serial number and the feature key did not match.	Ensure that the feature key being installed is specifically for this Switch serial number.
Invalid UDP port number.	UDP port number must be an integer from 1 through 65535.	Enter a port number from 1 through 65535.
Invalid value for BB_Credit.	BB_Credit must be an integer from 1 through 60.	Enter a number from 1 through 60.
Invalid value for day (1 - 31).	Value for day must be an integer from 1 through 31.	Enter a value from 1 through 31.
Invalid value for E_D_TOV.	Value for E_D_TOV must be an integer from 2 through 600, measured in tenths of a second.	Enter a value from 2 through 600.
Invalid value for hour (0 - 23).	Value for hour must be an integer from 0 through 23.	Enter a value from 0 through 23.
Invalid value for minute (0 - 59).	Value for minute must be an integer from 0 through 59.	Enter a value from 0 through 59.
Invalid value for month (1 - 12).	Value for month must be an integer from 1 through 12.	Enter a value from 1 through 12.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Invalid value for R_A_TOV.	Value for R_A_TOV must be an integer from 10 through 1200. Measured in tenths of a second.	Enter a value from 10 to 1200.
Invalid value for second (0 - 59).	Value for second must be an integer from 0 through 59.	Enter a value from 0 through 59.
Invalid value for year.	Value for year must be a four-digit year after 1980.	Enter a correct four-digit value for the year.
Invalid World Wide Name.	World Wide Name must have eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a World Wide Name using eight two-digit hexadecimal numbers separated by colons in the format given in the message.
Link dropped.	Connection between HAFM server and the Switch has been lost.	Wait for the connection to re-establish. Link re-connects are attempted every 30 seconds.
Log is currently in use.	Log is in use by another Product Manager.	Retry the operation later.
Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue.	External loopback diagnostics require an optical loopback plug to be installed.	Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing.
Maximum number of versions already installed.	The maximum number of firmware versions has been reached.	Delete a firmware version before adding a new firmware version.
No file was selected.	Action requires you to select a file	Choose a file.
No firmware version file was selected.	A file was not selected in the Firmware Library dialog box before an action, such as modify or send was performed.	Click a firmware version in the dialog box to select it, then perform the action again.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
No firmware versions to delete.	There are no firmware versions in the firmware library to delete.	N/A. An informational message.
Non-redundant switch must be offline to install firmware.	Since the Switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU.	Take Switch offline and try again.
Not all of the optical transceivers are installed for this range of ports.	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.
Performing this operation will change the current state to Offline.	This operation causes the Switch to go offline.	N/A. An informational message.
Performing this operation will change the current state to Online.	This operation causes the Switch to go online.	N/A. An informational message.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the Configure Date and Time dialog box, that the new time or date will overwrite the existing time or date set for the Switch.	Verify that you want to overwrite the current date or time.
Periodic Date/Time synchronization must be cleared before enabling switch clock alert.	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click Periodic Date/Time Synchronization check box in Configure Date and Time dialog box (Configure menu) to clear check mark and disable periodic date/time synchronization.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Port binding was removed from attached devices that are also participating in Switch Binding.	Informational message. User has removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.
Port cannot swap to itself.	Port addresses entered in the Swap Ports dialog box are the same.	Make sure that address in the first and second port address fields are different.
Port diagnostics cannot be performed on an inactive port.	This displays when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.
Port speeds cannot be configured at a higher rate than the director/switch speed.	This displays when you configure a port to 2 GB/sec and the Switch speed is set to 1 Gb/sec.	Set the port speed to 1 Gb/sec in the Configure Ports dialog box.
Product Manager error <number>.	The Switch Product Manager encountered an internal error and cannot continue.	Report the problem to support personnel.
Product Manager instance is currently open.	A Product Manager window is currently open.	Informational message only.
R_A_TOV must be greater than E_D_TOV.	R_A_TOV must be greater than E_D_TOV.	Change one of the values so that R_A_TOV is greater than E_D_TOV.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM server-to-product link is up. If the link is up, the HAFM server may be busy. Try the operation again later.
Send firmware failed.	Send firmware operation has failed.	Retry the operation. If the condition persists, contact support personnel.
SNMP trap address not defined.	An SNMP trap address must be defined if a community name is defined.	Define an SNMP address.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and Stop was selected on the Port Diagnostics dialog box. Diagnostics quit for the port for some reason, but the Stop button remains enabled.	Verify port operation. Retry diagnostics for port and choose Stop from the dialog box. If problem persists, contact your service representative.
Stop diagnostics failed. The test was not running.	The action to stop diagnostics failed because the test was not running.	Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the Director's Switch Membership List (SANtegrity Switch Binding feature), but you should note that one or more of these devices still has security control in port binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the Configure Ports dialog box.
Switch clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and user is attempting to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on Switches with failed ports.	Replace failed ports.
The add firmware process has been aborted.	User has ended the add firmware process.	N/A. An informational message.
The data collection process failed.	An error occurred in the data collection process.	Contact support personnel.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
The data collection process has been aborted.	User has ended the data collection process.	N/A. An informational message.
The default zone must be disabled to configure.	The message displays when the user attempts to change the operating mode to the open fabric mode and the default zone is enabled.	Disable the default zone and repeat the operation.
The HAFM server is busy processing a request from another Product Manager	The HAFM server could not process the current request because it is busy handling a request from another Product Manager.	Retry the operation later. If the condition persists, contact support personnel.
The firmware file is corrupted.	A firmware file has corrupt data.	Contact support personnel.
The firmware version already exists.	Firmware version already exists in the database.	N/A. An informational message.
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCNs.	User attempted to disable these parameters in the Configure Switch Parameters dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in HAFM, then disable the parameters
The IPL configuration cannot be deleted.	Deletion of the IPL address configuration was attempted and was not allowed.	Cancel the operation.
The link to the switch is not available.	The link from the HAFM server to the Switch is not available.	Check Ethernet connection.
The maximum number of address configurations has been reached.	The maximum number of saved address configurations has been reached.	Delete configurations no longer needed to allow new configuration to be saved.
The optical transceiver is not installed.	No information available for a port that is not installed.	Ensure the optical transceiver is installed and fully seated.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
The switch did not accept the request.	The Switch did not handle the action.	Try action again. If problem persists, contact your support representative.
The switch did not respond in the time allowed.	A time out was reached waiting for the Switch to respond to the action.	Try action again.
The switch is busy saving maintenance information.	Switch is busy with a maintenance operation.	Retry the operation later. If the condition persists, contact support personnel.
The switch must be offline to configure.	A configuration changed was attempted for a configuration requiring offline changes.	Take the appropriate actions to set the Switch offline before attempting the configuration change.
This feature has not been installed. Please contact your sales representative.	Indicator that the feature has not been installed on this Switch.	Contact your sales representative to obtain the desired feature.
This feature key does not include all of the features currently installed and cannot be activated while the switch is online	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the Switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the Switch offline through the Set Online State dialog box, then activate the new feature key using the Configure Feature Key dialog box.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported in firmware releases before 1.03.00.	Informational message.
Unable to change to incompatible firmware release.	The user tried to download a firmware release that is not compatible with the current product configuration.	Refer to the release notes or contact customer support.

Table A–1: StorageWorks Edge Switch 2/32 Product Manager Messages (Continued)

Message	Description	Action
Unable to save data collection file to destination.	Could not save data collection file to the specified drive (hard drive, network).	Retry the operation. If the condition persists, contact support personnel.
You do not have rights to perform this action.	User does not have the rights to perform this action.	An informational message.

Glossary

This glossary defines terms used in this guide or in other guides in this series, and is not a comprehensive glossary of computer terms.

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposite or substantively different meaning.

See. This refers the reader to another keyword or phrase for the same term.

See also. This refers the reader to definite additional information contained in another entry.

access control

List of all devices that can access other devices across the network and the permissions associated with that access. *See also* [persistent binding](#).

active FRU

A field-replaceable unit that is currently operating as the active and not the backup FRU.

active zone set

Single zone set that is active in a multiswitch fabric. It is created when you enable a specified zone set. This zone set is compiled by checking for undefined zones or aliases.

agent

Software that processes queries on behalf of an application and returns replies.

alarm

SNMP message notifying an operator of a network or device problem.

allowed port connection

In S/390 mode, this attribute establishes dynamic connectivity capability.

ANSI

American National Standards Institute: an organization that provides voluntary standards in the United States.

application-specific integrated circuit (ASIC)

A circuit designed for a specific application or purpose, such as implementing the lower-layer Fibre Channel protocol (FC-0). ASICs differ from general purpose devices such as memory chips or microprocessors.

alias server

Fabric software facility that supports multicast group management.

arbitrated loop

One of the three connection topologies offered by Fibre Channel. Up to 126 node ports and one fabric port can communicate without the need for a separate switched fabric. *See also* [point-to-point](#).

arbitration

Process of selecting one device from a collection of devices that request service simultaneously.

audit log

Log summarizing actions (audit trail) made by the user.

authentication

Verification of identity for a person or process.

backplane

The backplane provides 48 VDC power distribution and connections for all logic cards.

backup FRU

When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain Switch and Fibre Channel link operation.

beaconing

Use of light-emitting diodes on ports, port cards, field-replaceable units, and Switches to aid in the fault-isolation process; when enabled, active beaconing will cause LEDs to flash for faulty components.

BB_Credit

Also known as Buffer-to-Buffer Credit. Indicates the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device.

ber

See [bit error rate](#).

bidirectional

In Fibre Channel, the capability to simultaneously communicate at maximum speeds (100 Mbps) in both directions over a link.

bit error rate

A comparison of the number of bits received incorrectly by a device to the total number of bits transmitted.

blocked port

Devices communicating with the port are prevented from logging into the Switch or communicating with other devices attached to the Switch. A blocked port continuously transmits the offline sequence.

bridge

Device that connects and passes packets between two network segments that use the same communications protocol.

broadcast

Send a transmission to all N_Ports on a fabric.

broadcast frames

Data packet, also known as a broadcast packet, whose destination address specifies all computers on a network. *See also* [multicast](#).

buffer

Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See also* [BB_Credit](#).

CHPID

See [channel path identifier](#).

call-home

Product feature which enables the HAFM server to automatically dial out to a support center and report system problems. The support center server accepts calls from the HAFM server, logs reported events, and can notify one or more support center representatives.

channel

Point-to-point link that transports data from one point to the other.

channel path

A single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests.

channel path identifier

In a channel subsystem, a value assigned to each installed channel path of the system that uniquely identifies that path to the system.

channel wrap test

A diagnostic procedure that checks S/390 host-to-Switch connectivity by returning the output of the host as input. The test is host-initiated, and transmits Fibre Channel frames to a Switch port. A Switch port enabled for channel wrapping echoes the frame back to the host.

class of Fibre Channel service

Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

Class F Fibre Channel service

Used by Switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class 2 Fibre Channel service

Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two N_Ports. In-order delivery of frames is not guaranteed.

Class 3 Fibre Channel service

Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two N_Ports. Also known as datagram.

community profile

Information that specifies which management objects are available to what management domain or SNMP community name.

concurrent firmware upgrade

The CTP card provides two nonvolatile memory regions. Because two firmware versions can be stored on the card, firmware is upgraded without disrupting Switch operation. Note that the CTP card on this Switch is an internal component and not a FRU.

concurrent maintenance

Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units, while a hardware product is operating.

configuration data

Configuration data includes: identification data, port configuration data, operating parameters, SNMP configuration, and zoning configuration. A configuration backup file is required to restore configuration data if the CTP card in a nonredundant Switch or Switch is removed and replaced.

configuration report

An ASCII text file containing all current user-definable configuration options.

connectionless

Nondedicated link. Typically used to describe a link between nodes which allows the Switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this to the dedicated bandwidth that is required in a Class 1 Fibre Channel Service point-to-point link.

control processor card

Circuit card that contains the Switch microprocessor. The CTP card also initializes hardware components of the system after power-on. Note that the CTP card on this Switch is not a FRU.

control unit

A hardware unit that controls the reading, writing, or displaying of data at one or more input/output units.

control unit port

An internal port on the CTP card that communicates with the attached IBM S/390 or similar processor channels to report error conditions and link initialization.

CRC

See [cyclical redundancy check](#).

CTP

See [control processor card](#).

CUP

See [control unit port](#).

cyclical redundancy check

System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

DASD

Direct access storage device such as a disk drive.

data directory

Critical information for all managed products (including Directors and Switches). Information stored here includes: all HAFM configuration data (product definitions, user names, passwords, user rights, nicknames, session options, SNMP trap recipients, e-mail recipients, and Ethernet event notifications); all log files (HAFM logs and individual Product Manager logs); zoning library (all zone sets and zone definitions); firmware library; call-home settings (phone numbers and dialing options); configuration data for each managed Switch (stored on the HAFM server and in NVRAM on each Switch).

datagram

See [Class 3 Fibre Channel service](#).

default

Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.

default zone

Contains all attached devices that are not members of a separate zone.

destination address

Address identifier that indicates the targeted destination of a data frame.

device

Product, connected to a managed Switch, that is not controlled directly by the Product Manager. *See also* [node](#).

diagnostics

Procedures used by computer users and service personnel to diagnose hardware or software error conditions.

dialog box

Dialog box is a window containing informational messages or data fields to be modified or filled in with desired options.

D_ID

See [destination address](#).

Director

An intelligent Fibre Channel Switching device providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The Director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

DNS name

Domain name system or domain name service. Host or node name for a device or managed product that is translated to an IP address through a domain name server.

domain ID

Number (1 through 31) that uniquely identifies a Switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each Switch in the fabric by the principal Switch.

E_Port

See [expansion port](#).

E_D_TOV

See [error-detect time-out value](#).

embedded web server

A management interface embedded on the Switch's code which offers features similar to, but not as robust as, the HAFM and Product Manager.

error-detect time-out value

E_D_TOV defines the time the Switch waits for an expected response before declaring an error condition.

error message

Indication that an error has been detected. See also [information message](#) and [warning message](#).

Ethernet

A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the IEEE 802.3 standard, which specifies the physical and software layers. Baseband LAN allows multiple station access to the transmission medium at will without prior coordination and which avoids or resolves contention.

ethernet hub

A device used to connect the HAFM server and the Switches it manages.

event code

A numeric code that displays in the event log. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

event log

Record of significant events that have occurred on the Switch, such as FRU failures, degraded operation, and port problems.

expansion port

Physical interface on a Fibre Channel Switch within a fabric that attaches to an expansion port (E_Port) on another Fibre Channel Switch to form a multiswitch fabric. *See also* [segmented E_Port](#).

explicit fabric login

Data field size, supported by an F-Port, that is agreed upon during fabric login.

fabric

Entity that interconnects N_Ports and is capable of routing (switching) Fibre Channel frames using the destination ID information in the Fibre Channel frame header accompanying the frames.

fabric element

Any active Switch or node in a switched fabric.

fabric port

Physical interface within the fabric that connects to an N_Port through a point-to-point full duplex connection.

fabric services

Fabric services implements the various Fibre channel services that are described in the standards. These services includes the Fabric controller (login server), name server, and management server.

failover

Automatic and nondisruptive transition of functions from an active FRU that has failed to a backup FRU.

FCC-IOC

See [Fibre Channel I/O controller](#).

FE-MIB

See [Fibre Channel fabric element](#).

feature key

A string of alphanumeric characters consisting of both uppercase and lowercase. The following is an example of a feature key format: XxXx-XXxX-xxXX-xX.

fiber optics

Branch of optical technology concerned with the transmission of light pulses through fibers made of transparent materials such as glass, fused silica, and plastic.

fibre

Physical media types supported by the Fibre Channel specification, such as optical fiber, twisted pair, and coaxial cable.

Fibre Channel

Integrated set of standards recognized by ANSI which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel fabric element

Any device linked to a fabric. Information about these devices is recorded in a management information base (MIB) which can be accessed by fabric management software.

Fibre Channel I/O controller

Controls the embedded Fibre Channel port and configures the ports' ASICs.

fiber port module card

Each fiber port module card provides four Fibre Channel connections through duplex small form factor pluggable (SFP) fiber-optic transceivers.

FICON

An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium and significantly improves I/O performance (including one Gbps bidirectional data transfer)

FICON Management Server

An optional feature that can be enabled on the Director or Switch through the *Product Manager* application. When enabled, host control and management of the Director or Switch is provided through an S/390 Parallel Enterprise or zSeries Server attached to a Director or Switch port.

field-replaceable unit

Assembly removed and replaced in its entirety when any one of its components fails.

firmware

Embedded program code that resides and executes on the Switch.

FLASH memory

A computer chip with a read-only memory that retains its data when the power is turned off and that can be electronically erased and reprogrammed without being removed from the circuit board.

F_Port

See [fabric port](#).

FPM card

See [fibre port module card](#).

frame

A variable-length packet of data that is transmitted in frame relay technology.

FRU

See [field-replaceable unit](#).

gateway

A multi-homed host used to route network traffic from one network to another, and to pass network traffic from one protocol to another.

gateway address

A unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a gateway on the network.

GBIC

GigaBit Interface Converter. A removable module that converts an electrical serial data stream to an optical or amplified electrical serial data stream. Contains connector for attaching fiber optic cable.

generic port

Also known as G_Port. Physical interface on a Switch that can function either as a fabric port (F_Port) or an extension port (E_Port) depending on the port type to which it connects.

G_Port

See [generic port](#).

HAFM

High Availability Fabric Manager

HAFM Product Manager

The applications provide a graphical user interface (GUI) and management services, and implement web and other server functions.

HAFM server

PC shipped with a product to run the *HAFM* and *Product Manager* applications.

HAFM Management Services

Software application that provides back-end product-independent services to the *HAFM Manager* application. HAFM Management Services runs only on the HAFM Server (and cannot be downloaded to remote workstations).

hardware log

Record of FRU insertions and removals in the Switch.

hardware management console

The console runs the *Hardware Management Console* application (HWMCA), and is the operations and management PC platform for S/390 and zSeries servers.

HBA

See [host bus adapter](#).

heterogeneous fabric

A fabric with both HP and non-HP products.

homogeneous fabric

A fabric consisting of only HP products.

hop count

The number of hops a unit of information traverses in a fabric.

hexadecimal

A number system with a base of 16.

high availability

A performance feature characterized by hardware component redundancy and hot-swappability (enabling non-disruptive maintenance). High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

hop

Data transfer from one node to another node.

hop count

ISL connections.

host bus adapter

Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

hot-swapping

Removing and replacing a device's components while the device continues to operate normally.

hub

In Fibre Channel, a device that connects nodes into a logical loop by using a physical star topology.

IML

See [initial machine load](#).

inband management

Management of the Switch through Fibre Channel connection to a port card.

information message

Message telling a user that a function is performing normally or has completed normally. See also [error message](#) and [warning message](#).

initial machine load

Also known as IML. Hardware reset for the CTP card on the Switch. It does not affect other hardware. It is initiated by pushing the reset (RST) button on the machine's front panel.

initial program load

Process of initializing the device and causing the operating system to start. Initiated through a menu in the Product Manager.

input/output configuration

The collection of channel paths, control units, and I/O devices that attaches to the S/390 or zSeries processor.

input/output configuration program

A program that defines all available I/O devices and channel paths to an IBM S/390 or zSeries processor system. Replaced by the Hardware Configuration Definition Program starting with MVS/ESA Version 4.0.

interface

Hardware, software, or both, linking systems, programs, or devices.

Internet Protocol

The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an internet and provides the basis for connectionless, best-effort packet delivery service. IP includes the ICMP control and error message protocol as an integral part.

internet protocol address

Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability

Ability to communicate, execute programs or transfer data between various functional units over a network.

interswitch link

Also known as ISL. Physical E_Port connection between two Switches in a fabric.

I/O configuration

See [input/output configuration](#).

IOCDs

A data set that contains an I/O configuration definition built by the IOCP.

IOCP

See [input/output configuration program](#).

IP address

See [internet protocol address](#).

IPL

See [initial program load](#).

ISL

See [interswitch link](#).

jumper cable

Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable.

laser

Light Amplification through Stimulated Emissions of Radiation. A device that uses the oscillation of atoms or molecules between energy levels to generate a narrow, finely focused beam of light. The light has a single wavelength or narrow spectrum of wavelengths and is matched in phase and frequency.

latency

When used in reference to a Fibre Channel switching device, latency refers to the amount of time elapsed between receipt of a data transmission at a Switch's incoming F_Port (from the originating node port) to retransmission of that data at the Switch's outgoing F_Port (to the destination N_Port). The amount of time it takes for data transmission to pass through a switching device.

LED

Light-emitting diodes (LEDs) on Switch FRUs and the front bezel that provide visual indicators of hardware status or malfunctions.

LIN

See [link incident](#).

link

Physical connection between two devices on a switched fabric.

link incident

A link incident is a problem detected on a fiber optic link, like the loss of light, invalid sequences and other problems.

link incident alerts

A user notification, such as a graphic symbol in the hardware view that indicates that a link incident has occurred.

load balancing

Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on HP Switches takes place automatically.

log

A record, as of the performance of a machine or the progress of an undertaking.

logical port address

The port numbering system for a Switch with the FICON Management Server active.

logical unit number

Also known as LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's World Wide Name, represents a unique identifier for a logical device on a storage area network.

loopback plug

In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input.

loopback test

Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LUN

See [logical unit number](#).

MAC address

See [Media Access Control address](#).

maintenance port

Connector on the Switch operator panel where a PC running an ASCII terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product

Hardware product that can be managed with the Product Manager. For example, the Edge Switch 2/16 and Edge Switch 2/32 are managed products. *See also* [device](#).

management information base

Related set of software objects (variables) containing information about a managed device and accessed via SNMP from a network management station.

management session

Management session exists when a user logs on to the HAFM. HAFM can support multiple concurrent management sessions. The user must specify the network address of the HAFM's server at logon time.

Media Access Control address

Hardware address of a node (device) connected to a network.

MIB

See [management information base](#).

multicast

Delivery of a single transmission to multiple destination N_Ports. Can be one to many or many to many. All members of the group are identified by one IP address.

multiswitch fabric

Fibre Channel fabric created by linking more than one fabric switching device within a fabric.

name server

Program that translates names from one form into another. Domain name servers (DNS) translate domain names into IP addresses.

name server zoning

N_Port access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

network address

Name or address that identifies a managed product, such as the Edge Switch 2/16 and Edge Switch 2/32, on a TCP/IP network. The network address can be either an IP address in dotted-decimal notation (containing four three-digit octets in the format xxx.xxx.xxx.xxx), or a domain name (as administered on a customer network).

nickname

Alternate name assigned to a World Wide Name for a node or Switch in the fabric.

node

In Fibre Channel terminology, mode refers to an end device (server or storage device) that is or can be connected to a switched fabric.

node port

Physical interface within an end device which can connect to an F_Port on a switched fabric or directly to another N_Port (in point-to-point communications).

nondisruptive maintenance

Ability to service FRUs (including maintenance, installation, removal and replacement) while normal operations continue without interruption. *See also* [concurrent maintenance](#).

N_Port

See [node port](#).

offline sequence

Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so.

offline state

When the Switch is in the offline state, all the installed ports are offline. The ports transmit an OLS (offline sequence) and they cannot accept a login for connection from an attached device. *Contrast with* online state.

OLS

See [offline sequence](#).

online state

When the Switch is in the online state, all of the unblocked ports are allowed to login to the fabric and begin communicating. Devices can connect to the Switch if the port is not blocked and can communicate with another attached device if both devices are in the same zone or if the default zone is enabled. *Contrast with* offline state.

Open Systems Management Server

An optional feature that can be enabled on the Director or Switch through the *Product Manager* application. When enabled, host control and management of the Director or Switch are provided through an open systems interconnection (OSI) device attached to a Director or Switch port.

operating state (Switch)

The operating states are described as follows:

Online - when the Switch is set online, an attached device can log in to the Switch if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.

Offline - when the Switch is set offline, all ports are set offline. The Switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the Switch.

operating state (port)

Can be beaconing, invalid attachment, link incidents, link resets, no light, not operational, online, offline, segmented E_Port, port failure, or testing.

operating status (Switch)

Can be online, offline, coming online, or going offline.

optical cable

Fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications. See also [jumper cable](#), [optical cable assembly](#), and [trunk cable](#).

optical cable assembly

Optical cable that is connector-terminated. *See also* [optical cable](#).

See [optical fiber connector](#).

Circuit card that contains the Switch microprocessor. The CTP card also initializes hardware components of the system after power-on. A 10 Mbps RJ-45 twisted pair connector is located on the CTP card to connect to the Ethernet LAN and communicate with the HAFM server or a specific management station.

and optical cable.

optical fiber connector

Hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

out-of-band management

Transmission of management information using frequencies or channels other than those routinely used for information transfer.

packet

Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check), and frequently, user data.

panel

The main Product Manager window is divided into four view panels: title panel, menu bar, status bar, and view panel. Use features in these panels to configure Switch operation, monitor performance, and access maintenance features.

password

Unique string of characters known to the computer system and to a user who must specify it to gain full or limited access to a system and to the information stored within it.

path

In a network, any route between any two ports.

persistent binding

A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device) using a unit number.

point-to-point

A Fibre Channel topology which involves a dedicated link that connects only two stations. *See also* [arbitrated loop](#).

port

Receptacle on a device to which a cable leading to another device can be attached.

port name

Name that the user assigns to a particular port through the Product Manager.

POST

See [power-on self-test](#).

power-on self-test

Series of self-tests executed each time the unit is booted or reset.

preferred domain ID

Domain ID that a Switch is assigned by the principal Switch in a switched fabric. The preferred domain ID becomes the active domain ID except when configured otherwise by the user.

principal Switch

In a multiswitch fabric, the Switch that allocates domain IDs to itself and to all other Switches in the fabric. There is always one principal Switch in a fabric. If a Switch is not connected to any other Switches, it acts as its own principal Switch.

Product Manager

Application that implements the management user interface for the Switch.

product name

User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. For the Switch, the product name can also be accessed by an SNMP manager as the system name.

prohibited port connection

User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. For the Switch, the product name can also be accessed by an SNMP manager as the system name.

protocol

A standard procedure for regulating data transmission between computers.

PSP bucket

Preventive service planning bucket.

R_A_TOV

See [resource allocation time out value](#).

redundancy

Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hr./7 days per week) computer systems and networks.

redundant FRU

SFP LC transceivers, power supplies, and cooling fans that can be removed or replaced without disrupting Switch or Fibre Channel link operation.

remote access link

Connection to a device or program on a computer network via a (geographically) remote workstation.

remote notification

A process by which a system is able to inform remote users and/or workstations of certain classes of events that occur on the system. E-mail notification and the configuration of SNMP trap recipients are two examples of remote notification programs that can be implemented.

remote user workstation

Workstation, such as a PC, using HAFM and Product Manager software that can access the HAFM server over a LAN connection.

rerouting delay

Enabling rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new Switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

resource allocation time out value

R_A_TOV is a value used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

SAN

See [storage area network](#).

SC

Subscriber connectors.

segmented E_Port

E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. See also [expansion port](#).

SEL

System error light.

small form factor pluggable (SFP) transceivers

Laser-based optical transceivers for a wide range of networking applications requiring high data rates. The transceivers, which are designed for increased densities, performance, and reduced power, are well-suited for Fibre Channel applications.

simple mail transfer protocol

The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent, which stores and forwards the mail.

SMTP

See [simple mail transfer protocol](#).

SNMP

Simple Network Management Protocol. Specifies a mechanism for network management that is complete, yet simple. Information is exchanged between agents, which are the devices on the network being managed, and managers, which are the devices on the network through which the management is done.

SNMP community

Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

SNMP community name

The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

SNMP management station

An SNMP workstation console used to oversee the SNMP network.

SSP

See [system services processor](#)

status bar

This bar is at the bottom on the screen and displays a status symbol that indicates the current state of the Switch.

storage area network

A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

StorageWorks HA-fabric Manager

Software application that is the system management framework providing the user interface for managing HP Fibre Channel connectivity products. The HAFM can run both locally on the HAFM server and remotely on a user workstation.

subnet mask

A method of representing the portion of the IP network address that is devoted to subnet addresses (as opposed to the portions of the address that refer to individual hosts or to the organizational network overall).

switchover

Changing a backup FRU to the Active state, and the active FRU to the Backup state.

Switch priority

Value configured into each Switch in a fabric that determines its relative likelihood of becoming the fabric's principal Switch.

system services processor

Controls the RS-232 maintenance port and the Ethernet port of a Fibre Channel Switch.

topology

Logical and/or physical arrangement of stations on a network.

trap

Unsolicited notification of an event originating from a SNMP managed device and directed to an SNMP network management station.

trap host

SNMP management workstation that is configured to receive traps.

trunk cable

Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels and can be located within, or external to, a building. *Contrast with* jumper cable.

unblocked port

Devices communicating with an unblocked port can log in to the Switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

unicast

Communication between a single sender and a single receiver over a network. Compare to *multicast* (communication between a single sender and multiple receivers) and *anycast* (communication between any sender and the nearest of a group of receivers). Similar in meaning to *point-to-point communication*.

universal port module card

Each fiber port module card provides four Fibre Channel connections through duplex small form factor pluggable (SFP) fiber-optic transceivers. 1 or 2 gigabits per second enabled.

uniform resource locator

A standard way of specifying the location of an object, typically a web page, on the Internet. URLs are the form of address used on the World Wide Web. They are used in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer).

UPM card

See [universal port module card](#)

URL

See [uniform resource locator](#).

user rights

The HAFM's system administrator can assign levels of access, or "User Rights," to Product Manager users through the *HAFM* application.

vital product data

System-level data stored by the backplane in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

VPD

See [vital product data](#).

warning message

Indication that a possible error has been detected. *See also* [error message](#) and information message.

window

A scrollable viewing area on screen. A window may refer to a part of the application, such as the scrollable index window or the text window in the electronic versions of this database, or it may refer to the entire application in a window.

World Wide Names

Eight byte address that uniquely identifies a Switch, or a node (end device), even on global networks.

wrap plug

See [loopback plug](#).

WWN

See [World Wide Names](#).

zone

Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot.

zone member

Specification of a device to be included in a zone. A zone member can be identified by the port number of the Switch to which it is attached or by its device (or HBA) World Wide Name. In multiswitch fabrics, identification of end-devices/nodes by World Wide Name is preferable.

zone set

See [zone](#).

zoning

Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the Switch, may be configured into one or more zones. *See also* [zone](#).

Index

A

- active=saved 6-2
- alerts
 - threshold 1-19
- alerts, link incident (LIN) 2-39
 - enabling 3-10
- audit log 1-21, 4-3

B

- backing up and restoring
 - configuration 5-7
 - configuration data 3-37
- backup and restore configuration option 1-24
- bb_credit 3-8
- beaconing
 - enabling for ports 2-17
 - enabling for unit 2-14
- binding, port 2-19
- binding, ports 3-11
- block port option 2-17
- blocking a port 3-10

C

- call-home
 - notification, enabling 1-23
- call-home, enabling notification 5-6
- channel wrap option 2-18
- circle, green
 - meaning of 1-32
- clear link incident alert(s) option 2-18
- clear system error light
 - product menu 1-16
- close
 - product menu 1-16

- closing the product manager 1-33
- code pages 6-3
- collect maintenance data 5-2
- collecting maintenance data 5-2
- configuration data
 - backing up and restoring 3-37, 5-7
 - resetting 5-9
- configuration report 3-35
- configuration, resetting 5-9
- configurations
 - backing up and restoring 1-24
 - resetting 1-24
- Configure 3-21
- configure date and time dialog box 1-19, 2-14, 3-26, 3-27
- configure fabric parameters dialog box 3-6, 3-7
- configure feature key
 - dialog box 3-24
 - procedure 3-24
- configure feature key dialog box 1-19
- configure FICON management server dialog box 6-4
- configure identification dialog box 1-17, 3-2
- configure menu 1-16
 - configure threshold alert(s) 3-28
 - date/time 1-19
 - date/time option 3-26
 - enable telnet 1-20, 3-37
 - enable web server 1-20, 3-37
 - export configuration report 1-20, 3-35
 - features 1-19
 - identification 1-17
 - identification option 3-1

- operating parameters 1–17
- port # option 3–10
- ports 1–18
- SNMP agent 1–19
- SNMP option 3–22
- switch binding 1–18, 6–9
- threshold alert(s) 1–19
- configure open systems management server
 - dialog box 6–5
- configure operating parameters dialog box 1–17
- configure ports
 - open systems mode 3–12
- configure ports dialog box 1–18, 3–10
 - open systems mode 3–12
- configure SNMP dialog box 1–19, 3–22
- configure switch parameters dialog box 3–3
- configure threshold alerts, procedure 3–28
- configuring
 - date and time 1–19, 3–26
 - fabric operating parameters 3–6
 - identification 3–1
 - ports 3–10
 - SNMP
 - procedure 3–22
- configuring features, menu option 1–19
- customer-supplied server platform 1–1
- D**
- data collection option 1–22
- data speeds 3–11
- defaults
 - call-home notification 1–23
 - code page 6–3
 - enable e-mail notification 1–23
 - switch priority setting 3–9
- diagnostics (port), running 2–18, 5–1
- dialog boxes
 - configure date and time 2–14, 3–26, 3–27
 - configure fabric parameters 3–6, 3–7
 - configure feature key 1–19, 3–24
 - configure FICON management server 6–4
 - configure identification 1–17, 3–2
 - configure open systems management server 6–5
 - configure operating parameters 1–17
 - configure ports 1–18, 3–10, 3–12
 - configure SNMP 1–19, 3–22
 - configure switch parameters 3–3
 - export configuration report 1–20
 - firmware library 1–23
 - FRU properties 2–8
 - IPL confirmation 5–3
 - node properties 2–17
 - port diagnostics 1–22
 - port properties 1–26, 2–8, 2–16
 - port technology 2–17
 - save 4–2
 - save data collection 1–22
 - set online state 1–22
 - swap ports 5–1
 - switch binding membership list 6–9
 - switch properties 1–25, 2–12, 2–13
 - using 1–11
- diamond
 - fan module, meaning for 2–7
 - port connector, meaning for 2–6
 - power connector, meaning for 2–7
- diamond, red
 - meaning of 1–32
- director
 - fibre channel addresses 3–4
 - NVRAM 3–3, 3–6
- displaying
 - node properties 2–28
 - port statistics 2–32
- domain ID
 - insistent 3–5
 - preferred 3–4
- domain RSCNs
 - enterprise fabric mode 6–14

E

- e_d_tov 3–8
 - fabric segmentation 3–8
 - less than r_a_tov 3–8
 - multiswitch fabrics 3–8
- E_port segmentation
 - preferred domain ID 3–4
- EBCDIC code pages 6–3
- Edge Switch 2/32
 - date and time, configuring 3–26
 - managing 1–1
 - operational states 2–2
 - status 2–2
- Edge Switch 2/32 product manager
 - overview 1–11
- e-mail notification
 - enabling 1–23
- e-mail, enabling notification 5–6
- enable beaconing option 2–17
- enable call-home notification option 1–23, 5–6
- enable e-mail notification option 1–23
- enable management server (FICON) 6–2
- enable telnet 3–37
- enable telnet on switch 1–20
- enable unit beaconing
 - product menu 1–16
- enable web server 3–37
- enable web server on switch 1–20
- enabling e-mail notification 5–6
- enterprise fabric mode 6–13
- error light (ERR), clearing 2–14
- error statistics 2–34
- ethernet
 - no-link status 2–3
- event log 1–21, 4–5
- export configuration report
 - procedure 3–35
- export configuration report dialog box 1–20
- extended distance buffering (10–110 km) 3–10

F

- fabric binding 6–6
 - enterprise fabric mode 6–13
 - online state functions 6–7
- fabric parameters
 - bb_credit 3–8
 - e_d_tov 3–8
 - interop mode 3–9
 - r_a_tov 3–8
 - switch priority 3–8
- fabric segmentation
 - e_d_tov 3–8
 - preferred domain ID 3–4
- fans
 - identifying in hardware view 2–1
- feature
 - SANtegrity 6–6
- feature key 3–24
- fibre channel addresses 3–4
- FICON management server 3–6, 6–1
 - active=saved 6–2
 - code page 6–3
 - configuration procedure 6–4
 - configuring 6–2, 6–4
 - enable management server 6–2
 - host control 6–2
 - installing 6–1
 - programmed offline state control 6–2
- firmware
 - versions 5–5
- firmware library dialog box 1–23
- firmware versions 1–23
- frames too long, error statistics 2–35
- FRU
 - description 1–16
 - product menu 1–16
- FRU list view 1–28
 - defined 2–24
 - displayed 1–28, 2–24
 - opening 2–24
- FRU properties 2–8

H

- HAF manager, logging in 1–12
- HAFM manager
 - SMTP server address 1–23
- hardware log 1–21, 4–6
- hardware view 1–25
 - alert symbol function 1–25
 - displayed 1–25
 - displaying
 - port information 2–8
 - switch information 2–12
 - identifying FRUs 2–1
 - monitoring
 - component operation 2–1, 2–4
 - switch operation 2–2
 - obtaining
 - hardware status 2–8
 - information 2–8
 - status conditions 1–25
 - status table 2–2
 - switch menu 2–13
 - switch status table 2–2
 - using 1–25
 - using menus 2–13
- help
 - about option 1–24
 - contents option 1–24
- help menu 1–24
- host control 6–2
- host control prohibited field 6–4, 6–6

I

- icon
 - view 1–24
- identification, configuring for the switch 3–1
- If 2–29
- illustrations 1–11
- inband switch management 3–6
- initial program load (IPL) 1–22
 - executing 5–3
- insistent domain ID 3–4, 3–5
 - enterprise fabric mode 6–14

- interop mode 3–9
- invalid attachment messages 2–10
- IPL 1–22
 - executing 5–3
- IPL confirmation dialog box 5–3
- IPL switch 2–14

L

- languages, code page 6–3
- licensing information 1–11
- link incident (LIN) alerts 2–39
 - clearing 2–18
 - enabling 3–10
 - factory default 3–13
- link incident log 1–21
- logging in to HAFM manager 1–12
- login
 - password 1–1, 1–12
 - username 1–1, 1–12
- logs
 - audit 1–21, 4–3
 - event 1–21, 4–5
 - expanding columns 4–2
 - hardware 1–21, 4–6
 - link incident 1–21
 - threshold alert 4–8
 - using 4–1
 - window button function 4–1
- logs menu 1–20
 - audit 1–21
 - event 1–21
 - hardware 1–21
 - link incident 1–21

M

- maintenance data, collecting 5–2
- maintenance menu 1–22
 - backup and restore configuration 1–24
 - backup and restore configuration option 3–37, 5–7
 - collect maintenance data option 5–2
 - data collection 1–22
 - enable call-home notification 1–23

- enable call-home notification option 5–6
- enable e-mail notification 1–23
- enable e-mail notification option 5–6
- firmware library 1–23
- IPL 1–22
- IPL option 5–3
- port diagnostics 1–22
- port diagnostics option 5–1
- reset configuration 1–24
- reset configuration option 5–9
- set online state 1–22
- set online state option 5–4
- management
 - SNMP agent 1–2
- management server
 - FICON 6–1
 - configuring 6–2
 - installing 6–1
 - open systems 6–5
 - installing 6–5
- managing the Edge Switch 2/32 switch,
 - introduction 1–1
- menu bar, description 1–15
- menus
 - configure 1–16
 - hardware view 2–13
 - help 1–24
 - logs 1–20
 - maintenance 1–22
 - menu bar 1–15
 - node list view 1–29
 - performance view 1–31, 2–30
 - port 1–26, 2–16
 - port list view 1–27, 2–23, 2–27
 - product 1–15
 - switch 1–25, 2–13
- mode
 - enterprise fabric 6–13
 - interop 3–9
 - open fabric 1.0 3–9
 - open systems 3–6
 - S/390 3–6

- multiswitch fabric
 - e_d_tov 3–8
 - principal switch 3–8

N

- node list view 1–29, 2–25
- node list view menu 1–29
- node properties dialog box 2–17
- node properties, displaying 2–28
- no-link status 2–3
- NVRAM 3–3, 3–6

O

- online state, setting 5–4
- open fabric 1.0 3–9
- open systems management server 6–5
 - configuring 6–5
 - installing 6–5
- open systems mode 3–6
 - identifying port numbers 3–10
 - naming ports 3–10
 - port type 3–11
- operating parameters
 - rerouting delay 3–5
- operating states for ports 2–36

P

- password, default 1–1, 1–12
- performance view 2–30
- performance view menu 1–31, 2–30
- performance view option 1–30
- port
 - description 1–15
- port binding 2–19, 3–11
- port diagnostics dialog box 1–22
- port list view 2–21
 - displayed 1–27, 2–21
 - menus 2–23, 2–27
 - opening 2–21
- port list view menu 1–27
- port menu 1–26, 2–16
- port operating states 2–36

- port properties dialog box 1–26, 2–8, 2–16
 - reason field messages 2–10
- port statistics
 - class 2 statistics 2–33
 - class 3 statistics 2–34
 - error statistics 2–34
 - traffic statistics 2–32
- port technology dialog box 2–17
- ports
 - attention indicator 2–5
 - beaconing or diagnostic test 2–6
 - binding 2–19, 3–11
 - blocking 2–17, 3–10
 - configuring 1–18, 3–10
 - open systems mode 3–12
 - data speed 3–11
 - default configuration 1–18
 - diagnostics 1–22, 2–18, 5–1
 - displaying statistics 1–31, 2–32
 - extended distance buffering (10–110 km) 3–10
 - failure indicator 2–6
 - identifying in hardware view 2–1
 - LEDs 2–6
 - menu 2–16
 - naming 3–10
 - operating states 2–36
 - product menu 1–15
 - resetting 2–18
 - statistics description 2–32
 - type 2–23
 - WWN binding 2–19
- ports list view 1–27
- power indicator 2–6
- power supplies
 - identifying in hardware view 2–1
- preferred domain ID 3–4
 - multiswitch fabric 3–3, 3–7
- principal switch, determining 3–8
- procedure
 - collect maintenance data 5–2
- product manager 1–25
 - closing 1–33
 - configure 1–16
 - FRU list view 1–28, 2–24
 - hardware view 2–1
 - help menu 1–24
 - licensing 1–11
 - logs menu 1–20
 - maintenance menu 1–22
 - menu bar 1–15
 - node list view 1–29, 2–25
 - node list view menu 1–29
 - non-English language support 6–3
 - overview 1–11
 - performance view 1–30, 2–30
 - performance view menu 1–31
 - port list view 1–27, 2–21
 - port menu 1–26
 - product 1–15
 - status bar 1–32
 - switch view 1–25
 - user rights 1–34
 - view panel 1–25
 - view tabs 1–24
 - window layout and function 1–15
- product menu 1–15
 - clear system error light 1–16
 - close 1–16
 - enable unit beaconing 1–16
 - FRU 1–16
 - port 1–15
 - ports 1–15
 - properties 1–16
- programmed offline state control 6–2
- properties
 - product menu 1–16

R

- r_a_tov 3–8
 - greater than e_d_tov 3–8
- reason field messages 2–10
- remote user workstations 1–8
- rerouting delay 3–5
 - enterprise fabric mode 6–13
- reset configuration option 1–24
- reset ports option 2–18
- resetting
 - configuration 5–9
 - configuration data 5–9
- rights for product manager users 1–34

S

- S/390 mode
 - FICON management server 3–6
- SANtegrity feature 6–6
 - fabric binding 6–6
- SANtegrity features
 - switch binding 6–7
- save data collection dialog box 1–22
- save dialog box 4–2
- segmented E_Port messages 2–11
- server platform
 - customer-supplied 1–1
- set online state dialog box 1–22
- setting online state 5–4
- signal losses, error statistics 2–34
- SMTP server address 1–23
- SNMP
 - configuring 3–22
 - introduction 1–2
- SNMP agent option 1–19
- software licensing 1–11
- speeds, port 3–11
- square, gray, meaning of 1–32
- statistics on ports 1–31, 2–32
- status bar 1–32
 - status symbols 2–4

- status symbols 2–4
- status table 2–2
- swap ports
 - dialog box 5–1
- switch
 - displaying information 2–12
- switch binding 6–7, 6–13
 - configuring 3–24
 - enable and disable 6–8
 - membership list 6–9
 - online state functions 6–11
 - zoning function 6–12
- switch binding membership list dialog box 6–9
- switch clock alert mode 6–2
- switch clock alert mode field 6–4
- switch menu 1–25
- switch parameters
 - insistent domain ID 3–5
 - NVRAM storage 3–3, 3–6
 - preferred domain ID 3–4
- switch priority 3–8
 - related number codes 3–9
- switch priority setting 3–9
- switch properties 2–13
- switch properties dialog box 1–25, 2–12, 2–13
- switch status 2–4
- switch status table 2–2
- switches, principal, determining 3–8
- system error indicator 2–6

T

- telnet, enabling 3–37
- threshold alert
 - configuring 3–28
 - log 4–8
 - port properties dialog box 2–10
- threshold alerts 1–19
- triangle, port, meaning for 2–5
- triangle, yellow
 - meaning of 1–32

U

unit beaconing indicator 2–6
United States/Canada 00037 code page 6–3
user rights 1–34
username, default 1–1, 1–12

V

versions, firmware 1–23
view menu
 FRU list view 2–24
 node list view 2–25

performance view 2–30

port list view 2–21

view panel 1–25

view tabs 1–24

W

web server, enabling 1–20, 3–37

WWN

 principal switch 3–8

WWN binding 3–11

WWN binding option 2–19